PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-225143
(43)Date of publication of application : 17.08.1999

(51)Int.CI. H04L 9/32
G06F 17/60
G06K 17/00
G07B 1/00
G07B 5/00
G07F 7/12
G09C 1/00

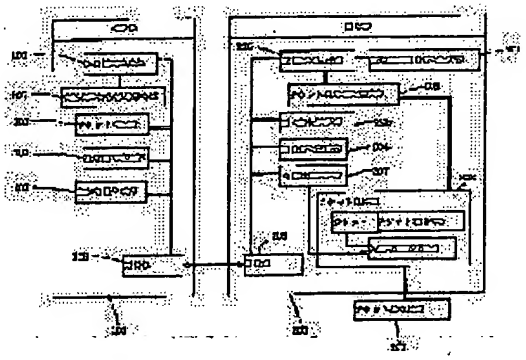
AB

(21)Application number : 10-027074
(22)Date of filing : 09.02.1998

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : KIKO KENICHIROU
NAKAGAKI JUHEI
KIYOUJIMA HITOKI
TANIGUCHI SHINICHIRO

(54) ELECTRONIC TICKET SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent an internal state of a certificate device from being revised due to a ticket exhibited by mistake or illegally.
SOLUTION: An authentication information generating section 102 of an authentication device 100 generates authentication information and sends it to a certificate device 200. A ticket discrimination information generating section 203 of the certificate device 200 generates ticket discrimination information to indicate storage of a correct ticket from ticket utilization information and information in an internal state storage area. A certificate information generating section 206 connects ticket discrimination information to low-order bits of a bit stream of the authentication information to generate ticket certificate information. The ticket certificate information is sent to the authentication device 100 by a communication section 208. The authentication device 100 receiving the ticket certificate information conducts ticket discrimination processing and terminates the protocol when the ticket certificate information is incorrect or the ticket is not to be authenticated.



LEGAL STATUS

[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１１－２２５１４３

(43)公開日　平成１１年（１９９９）８月１７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04L 9/32			H04L 9/00	675 D	
G06F 17/60			G06K 17/00	T	
G06K 17/00				S	
			G07B 1/00	A	
G07B 1/00				B	

審査請求　未請求　請求項の数４１　ＯＬ　（全２９頁）　最終頁に続く

(21)出願番号　特願平１０－２７０７４

(22)出願日　平成１０年（１９９８）２月９日

(71)出願人　０００００５４９６
富士ゼロックス株式会社
東京都港区赤坂二丁目１７番２２号

(72)発明者　木子　健一郎
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　京嶋　仁樹
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

(74)代理人　弁理士　澤田　俊夫

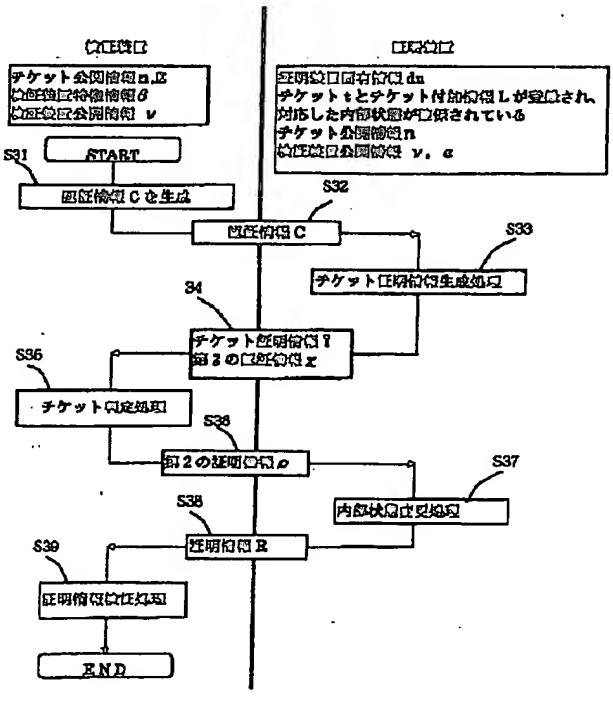
最終頁に続く

(54)【発明の名称】電子チケットシステム

(57)【要約】

【課題】　誤って、または不正に提示されたチケットにより証明装置の内部状態が変更されないようにする。

【解決手段】　検証装置１００の認証情報生成部１０２が、認証情報Ｃを生成し証明装置２００に送る（Ｓ３１、Ｓ３２）。証明装置２００のチケット判定情報生成部２０３は、正しいチケットを保持していることを示すためのチケット判定情報Ｍを、チケット利用情報および内部状態記憶領域の情報から生成する。証明情報生成部２０６は、認証情報Ｃのビット列の下位にチケット判定情報Ｍを連結し、チケット証明情報Ｔを生成する（Ｓ３３）。チケット証明情報Ｔは、通信部２０８により検証装置１００に送られる（Ｓ３４）。Ｔを受け取った検証装置１００はチケット判定処理を行い、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないものの場合には、プロトコルを終了する（Ｓ３５）。



実施例１の処理全体のフローチャート

1

【特許請求の範囲】

【請求項１】　証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、

上記証明装置は、

上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、

上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとからチケット秘密情報を生成し、上記チケット秘密情報を用いて証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するチケット判定手段と、

上記証明装置がチケット秘密情報を生成できたか否かを、上記証明情報に基づいて、検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項２】　請求項１に記載の電子チケットシステムであって、

上記検証装置は、対話証明で用いられる認証情報を生成する認証情報生成手段を有し、

上記証明装置の証明情報生成手段は、上記検証装置が生成した認証情報を用いて上記証明情報を生成する電子チケットシステム。

【請求項３】　請求項２に記載の電子チケットシステムであって、上記証明装置と上記検証装置とは通信手段を有し、上記証明装置は証明しようとするチケットのチケット判定情報を、上記検証装置に伝達する電子チケットシステム。

【請求項４】　請求項２ないし３に記載の電子チケットシステムであって、

上記電子チケットシステムは、上記検証装置と上記証明装置とに加えて、チケット発行装置を有し、

上記チケット発行装置は、

発行するチケットの秘密の特徴情報である上記チケット秘密情報と対応するチケット公開情報を保持するチケット特徴情報保持手段と、

利用者が保持する上記証明装置の固有情報を保持するチケット発行用証明装置固有情報保持手段と、

上記チケット特徴情報保持手段に保持している上記チケット秘密情報と、上記チケット発行用証明装置固有情報保持手段に保持している上記証明装置固有情報とを用いて、デジタル情報であるチケットを作成するチケット発行手段ををを有する電子チケットシステム。

【請求項５】　請求項２ないし４の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少なくとも上記検証装置から送られた認証情報と、上記チケットと、上記チケット判定情報と、上記証明装置固有情報とより所定の方法で、上記証明情報の１つとして、上記チケット判定手段の判定に用いるチケット証明情報を計算する電子チケットシステム。

2

【請求項６】　請求項５に記載の電子チケットシステムであって、上記証明装置はチケットの利用条件を定めたチケット利用情報を、チケットと対応させて上記チケット保持部に保持する電子チケットシステム。

【請求項７】　請求項５に記載の電子チケットシステムであって、上記証明装置は、上記チケット判定情報を作成する際に、少なくとも上記チケット利用情報を用いる電子チケットシステム。

【請求項８】　請求項６に記載の電子チケットシステムであって、上記証明装置は、可変な内部状態を保持する内部状態記憶領域と、上記内部状態の値を制御する内部状態制御手段とを備える電子チケットシステム。

【請求項９】　請求項８に記載の電子チケットシステムであって、上記証明装置のチケット判定情報生成手段は、上記チケット判定情報を作成する際に、少なくとも上記証明装置の内部状態記憶領域の情報を用いる電子チケットシステム。

【請求項１０】　請求項８ないし９の電子チケットシステムであって、上記証明装置の内部状態記憶領域が保持する可変な内部状態のうちの、少なくとも一部は外部から書き換え不能である電子チケットシステム。

【請求項１１】　請求項８ないし１０の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少なくとも、上記チケットと、上記チケット利用情報と、上記証明装置固有情報とを用いて上記証明情報を計算する電子チケットシステム。

【請求項１２】　請求項８ないし１１の電子チケットシステムであって、上記証明装置は、上記検証手段から送られた上記認証情報を保持する認証情報保持手段を有し、上記証明情報生成手段は、上記チケット判定情報生成手段により生成されたチケット判定情報を用いて、上記認証情報保持手段に保持されている認証情報を変更して上記証明情報の生成に利用する電子チケットシステム。

【請求項１３】　請求項１２の電子チケットシステムであって、上記チケット判定情報生成手段が生成したチケット判定情報をＭとし、上記認証情報をＣとすると、上記証明装置の証明情報生成手段は、上記認証情報保持手段に保持されている認証情報Ｃを、ＣにＭを接合したものに更新する電子チケットシステム。

【請求項１４】　請求項１２ないし１３の電子チケットシステムであって、上記証明装置の証明情報生成手段は、上記証明情報の１つとしてチケット証明情報を生成することが可能であり、上記チケット証明情報は、上記チケットと、上記チケット利用情報と、上記証明装置固

有情報とより所定の方法でチケット秘密情報を計算し、上記認証情報に対して、チケット秘密情報を用いた計算を施すことによって生成される電子チケットシステム。

【請求項15】　請求項14の電子チケットシステムであって、p、qが素数であり、n＝p・qであり、DE≡1　mod　(p－1)(q－1)の関係が満たされるとき、上記チケット秘密情報がDであり、チケット公開情報が(n，E)であり、上記チケット利用情報がLであり、上記証明装置固有情報が秘密の値duであり、f(du，L，n)を一方向性関数として、チケットがt＝D－f(du，L，n)で与えられているとき、上記証明装置の証明情報生成手段は、上記認証情報C(上記証明情報生成手段が変更した認証情報)に対して、Cの法nでのtによる冪乗と、Cの法nでの一方向性関数値f(du，L，n)による冪乗との法nでの積$C'C^{''((du,L,n))}$ mod nとしてチケット証明情報を計算する電子チケットシステム。

【請求項16】　請求項14の電子チケットシステムであって、p、qが素数であり、n＝p・qであり、DE≡1　mod　(p－1)(q－1)の関係が満たされるとき、上記チケット秘密情報がDであり、チケット公開情報が(n，E)であり、上記チケット利用情報がLであり、上記証明装置固有情報が秘密の値duであり、f(du，L，n)を一方向性関数として、上記チケットがt＝D－f(du，L，n)で与えられているとき、上記証明装置は、あらかじめt＋f(du，L，n)＝Dを計算し、その値を用いて、上記認証情報C(上記証明情報生成手段が変更した認証情報)に対して、$T=C^{D}$ mod nとしてチケット証明情報Tを計算する電子チケットシステム。

【請求項17】　請求項14の電子チケットシステムであって、gが離散対数問題が困難な群の原始根であり、pが素数であり、整数xに対してy＝g'mod pが成り立つとき、上記チケット秘密情報がxであり、チケット公開情報が(y，p，g)であり、上記チケット利用情報がLであり、上記証明装置固有情報が秘密の値duであり、f(du，L，y)を一方向性関数として、上記チケットがt＝x－f(du，L，y)で与えられているとき、上記証明装置は、上記認証情報C(上記証明情報生成手段が変更した認証情報)に対して、上記チケット判定情報TをCの法pでのtによる冪乗と、Cの法pでの一方向性関数値f(du，L，y)を指数とする冪乗との法pでの積$C'C^{''((du,L,y))}$ modnとして上記証明情報を計算する電子チケットシステム。

【請求項18】　請求項14の電子チケットシステムであって、gが離散対数問題が困難な群の原始根であり、pが素数であり、整数xに対してy＝g'mod pが成り立つとき、上記チケット秘密情報がxであり、チケット公開情報が(y，p，g)であり、上記チケット利用情報がLであり、上記証明装置固有情報が秘密の値d

uであり、f(du，L，y)を一方向性関数として、上記チケットがt＝x－f(du，L，y)で与えられているとき、上記証明装置は、あらかじめt＋f(du，L，y)＝xを計算し、上記認証情報Cに対して(上記証明情報生成手段が変更した認証情報)チケット判定情報Tを計算する際に、C' mod pの値を用いる電子チケットシステム。

【請求項19】　請求項14ないし18の電子チケットシステムであって、上記検証装置の証明情報検証手段は、上記認証情報生成手段が作成した認証情報と、上記証明装置から送られたチケット証明情報と、上記チケット公開情報とより、上記チケット証明情報の正当性を検証し、上記チケット証明情報が正しい場合は、上記チケット証明情報に埋め込まれたチケット判定情報を導出する電子チケットシステム。

【請求項20】　請求項19の電子チケットシステムであって、上記認証情報がCであり、上記チケット証明情報がTであり、上記チケット公開情報(n、E)であり、あるビット列Mがある場合に、上記検証装置の証明情報検証手段は、上記チケット証明情報Tを法nでEでべき乗したものをCとMとを接合したビット列と比較し、T^{E} mod n＝C||M(記号||はビット列の接合)となっていれば、上記チケット証明情報は正しいと判定し、上記チケット証明情報が正しい場合はMを上記チケット判定情報として導出する電子チケットシステム。

【請求項21】　請求項19の電子チケットシステムであって、上記認証情報がCであり、上記チケット証明情報がTであり、上記チケット公開情報が(p，g，y)である場合に、上記検証装置の証明情報検証手段は、自身が発生させた乱数をrとするとき、あるビット列Mがあって、T／y' mod p＝(C||M)　(記号||はビット列の接合)となっていれば、上記チケット証明情報は正しいと判定し、上記チケット証明情報が正しい場合はMをチケット判定情報として導出する電子チケットシステム。

【請求項22】　請求項8ないし21の電子チケットシステムであって、

上記証明装置は、上記検証装置を認証するための第2の認証情報を生成する、第2の認証情報生成手段と、上記検証装置が生成する第2の証明情報を検証するための、第2の証明情報検証手段とを有し、

上記第2の証明情報検証手段は、上記第2の認証情報と、上記第2の証明情報と、チケット公開情報とより上記第2の証明情報が正しいかどうかを検証し、

上記第2の証明情報が正しい場合、上記内部状態制御手段は、上記証明装置の内部状態を変更する電子チケットシステム。

【請求項23】　請求項22の電子チケットシステムであって、上記検証装置の証明情報検証手段は、上記チケ

5

ット判定手段による判定の結果をもとにして、上記第２の証明情報を生成するか否かを決定する電子チケットシステム。

【請求項２４】　請求項２２の電子チケットシステムであって、

上記証明装置は、チケットのカウンタとして機能する内部状態をチケットと関連づけ、外部から書き換え不能な形で、内部状態記憶領域に保持し、

上記検証装置の証明情報検証手段は、上記証明装置から送られたチケット判定情報に含まれる内部状態のカウンタの値が、所定の値であるときには、対応するチケットが無効であるものと判断する電子チケットシステム。

【請求項２５】　請求項２２ないし２４の電子チケットシステムであって、ｐ'、ｑ'が素数であり、$\nu = p' \cdot q'$であり、$\delta\varepsilon \equiv 1 \mod (p'-1)(q'-1)$の関係が満たされるときに、上記証明装置の第２の証明情報検証手段は、上記第２の認証情報χと上記第２の証明情報ρが、

【数１】

$$\chi = \rho^{\varepsilon} \mod \nu$$

を満たす場合に上記第２の証明情報が正しいと判定する電子チケットシステム。

【請求項２６】　請求項２２ないし２４の電子チケットシステムであって、ｇが離散対数問題が困難な群の原始

$\chi \| \mu = \rho^{\varepsilon} \mod \nu$（記号||はビット列の接合）

を満たすときに、上記第２の証明情報が正しいと判定し、μを上記第２の証明情報に埋め込まれた情報として導出する電子チケットシステム。

【請求項３０】　請求項２７の電子チケットシステムであって、上記証明装置の内部状態制御手段は、上記第２の証明情報から導出された情報にもとづいて上記内部状態記憶領域に保持された内部状態を変更する電子チケットシステム。

【請求項３１】　請求項３０の電子チケットシステムであって、上記証明装置の上記第２の証明情報検証手段は、上記検証装置より送られた内部状態変更を許可する情報と、内部状態とに基づいて、上記証明情報を正しく生成するか否かを判定する電子チケットシステム。

【請求項３２】　請求項２２ないし３１の電子チケットシステムであって、上記検証装置は、上記検証装置の特権を表す秘密情報である、検証装置特権情報を保持する検証装置特権情報保持部と、上記第２の証明情報を生成する第２の証明情報生成部を有し、

上記第２の証明情報生成部は、上記第２の認証情報と上記検証装置特権情報とより第２の証明情報を生成する電子チケットシステム。

【請求項３３】　請求項３２の電子チケットシステムであって、上記検証装置特権情報をδとし、対応する公開情報を（ν，ε）とするとき、上記検証装置の第２の証明情報生成部は、上記第２の認証情報χより上記第２の

6

根であり、ｐが素数であり、整数ξに対して

【数２】

$$\eta = g^{\xi} \mod p$$

が成り立つときに、証明装置の第２の認証情報生成手段は、乱数ｒ'と上記第２の認証情報$\chi = g^{r'}$を生成し、上記第２の証明情報検証手段は上記第２の証明情報ρについて、$\rho / \eta^{r'} \mod p = \chi$が満たされた場合に上記第２の証明情報が正しいと判定するる電子チケットシステム。

【請求項２７】　請求項２２の電子チケットシステムであって、上記証明装置の第２の証明情報検証手段は、上記第２の証明情報が正しい場合は、上記第２の証明情報に埋め込まれた情報を導出する電子チケットシステム。

【請求項２８】　請求項２７の電子チケットシステムであって、上記証明装置の第２の証明情報検証手段は、上記第２の証明情報から導出された情報を、上記内部情報の変更を許可するための情報として利用する電子チケットシステム。

【請求項２９】　請求項２７ないし２８の電子チケットシステムであって、チケット公開情報はνおよびεを含んでおり、上記証明装置の第２の証明情報検証手段は、上記第２の認証情報χと上記第２の証明情報ρとが、あるビット列μに対して、

【数３】

$\chi \| \mu = \rho^{\varepsilon} \mod \nu$（記号||はビット列の接合）

証明情報ρを

【数４】

$$\rho = \chi^{\delta} \mod \nu$$

として生成する電子チケットシステム。

【請求項３４】　請求項３２の電子チケットシステムであって、上記検証装置特権情報をξ、対応する公開情報を（ｐ，ｇ，η）とし、

【数５】

$$\eta = g^{\xi} \mod p$$

の関係が満たされるとき、上記検証装置の第２の証明情報生成部は上記第２の認証情報χに対して、

【数６】

$$\chi^{\xi} \mod p$$

の値を用いて上記第２の証明情報ρを生成する電子チケットシステム。

【請求項３５】　請求項３２ないし３４の電子チケットシステムであって、上記検証装置は上記第２の認証情報を保持する、第２の認証情報保持部を有し、上記検証装置の第２の証明情報生成部は、上記検証装置特権情報を用いた計算を施す際に、証明装置の内部状態の変更を許可する情報と、上記第２の認証情報より上記第２の証明情報を計算する電子チケットシステム。

【請求項３６】　請求項３２ないし３４の電子チケットシステムであって、上記検証装置の第２の証明情報生成部は、上記検証装置特権情報を用いた計算を施す前に、

7

上記証明装置の内部状態の変更を許可する情報を用いて、上記第２の認証情報保持部に保持された上記第２の認証情報を更新する電子チケットシステム。

【請求項３７】　請求項３６の電子チケットシステムであって、上記検証装置の第２の証明情報生成部は、上記証明装置の内部状態の変更を許可する情報をμとし、上記第２の認証情報をχとすると、上記第２の認証情報保持部に保持された第２の認証情報をχにμを接合したものに更新する電子チケットシステム。

【請求項３８】　請求項１ないし３７に記載の電子チケットシステムであって、少なくとも、上記証明装置が、内部のデータ及び処理手続きを外部から観測することを困難ならしめる防御手段中に保持されている電子チケットシステム。

【請求項３９】　請求項ないし３７に記載の電子チケットシステムであって、少なくとも、上記証明装置が、ＩＣカードなどの携帯可能な小型演算装置として構成されている電子チケットシステム。

【請求項４０】　証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、

上記証明装置は、

上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、

上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとから証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するチケット判定手段と、

上記証明装置が上記証明装置固有情報と上記チケットから上記証明情報を生成できたか否かを検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項４１】　検証装置と電子チケットを保持する認証装置との間で相互認証を行ないながら検証装置側で所定のサービスを実行し、認証装置側で内部状態を変更する電子チケット利用方法において、

上記証明装置が、上記電子チケットの権利内容または上記電子チケットの使用状態を表すチケット判定情報を上記検証装置に提示するステップと、

上記検証装置が、提示された上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するステップとを有することを特徴とする電子チケット利用方法。

【発明の詳細な説明】

【０００１】

8

【発明の属する技術分野】本発明は、チケットやカードを電子的に作成し利用する技術に関する。

【０００２】

【背景の技術】［従来の技術］近年、乗車券、入場券、指定券、予約券、回数券、定期券、プリペイドカード、ポイントカード、などの一般的なチケットを、電子チケットとして発行する試みが行われている。

【０００３】このような電子チケットは、発行者が、利用者に与えた権利を特定でき、正しいチケットであることを検証できるという機能を持つ。電子情報は、作成が容易であり、通信回線を通して送信できるという特長を持つが、完全なコピーを簡単に作れるので、電子チケットの実現には、偽造と複製による不正利用への対策が不可欠である。電子署名により偽造の防止は可能だが、複製の防止は困難であり、複製による不正利用を防止することが、電子チケットの実現にあたっての最大の課題となっていた。

【０００４】この問題に対する、解決策として、従来、チケットの利用時に正当な利用者か確認する第１の従来技術、発行者以外の者にチケットを複写する機会を与えない第２の従来技術、検証時の通信を公開できるように第２の従来技術を修正した第３の従来技術の、３つの方法が提案されてきた。

【０００５】第１の従来技術は、チケットの利用時に利用者が、正当な利用者かどうかを確認する方法であり、利用者は、チケットを利用する時に、チケットとともに、自分が利用者特定情報に適合する正当な利用者であることを示す。利用者特定情報に適合していれば、対応する権利の行使が認められる。確認のために必要な情報（利用者特定情報）と、与えた権利とを対応づける情報がチケットとして発行され、利用者が記録管理する。発行者以外の者が勝手にチケットを偽造できないようにするためには、発行者がチケットに電子署名を施す。電子署名のないチケットは、偽造されたものと判断される。利用者特定情報には、身元、顔写真などの身体的特徴、パスワードなどの知識の所有などが利用できる。

【０００６】しかしながら、この方法では、利用する利用者特定情報に応じて、いくつかの問題点が生ずる。

【０００７】例えば、利用者特定情報に利用者の身元を利用する方法では、発行時と検証時に利用者の身元が明らかになり、匿名性が失われてしまう。また、通信回線を利用した遠隔的な環境で身分を安全に証明する方法は実現されていないので、このような環境では正当な権利を持たないものが、不当にチケットを利用することを防止することができない。

【０００８】利用者特定情報にパスワードを利用すれば、匿名性の問題は軽減されるが、パスワードを記憶する負荷を利用者に与える。また、利用者が故意にパスワードを漏洩させることを防止できないので、不正利用の危険が増してしまうという問題点もある。

【０００９】第２の従来技術は、例えば特開平８－１４７５００号公報に示されるようなものであり、発行者以外の者にチケットを複写する機会を与えない方法である。この方法では、利用者が保持管理しているチケットを複写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。

【００１０】しかしながら、この方法では

（１）発行者以外の者はチケットを複写できないので、チケットの正当性を第三者に証明することが困難になる、（２）チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できない、といった問題点が生ずる。

【００１１】第３の従来技術は、例えば特公平６－５２５１８号公報に示されるようなものであり、検証時の通信を公開できるように、第２の従来技術を修正した方法である。この方法では、第２の従来技術と同様に、チケットを秘密情報として利用者の所持する装置（証明装置）に複写できないように記録するが、検証の方法が異なっている。まず、検証を行う検証装置は、証明装置に乱数などの繰り返し利用されない値（チャレンジ）を送る。証明装置は、チケットである秘密情報を利用した演算をチャレンジに対して施して、得られた値（レスポンス）を検証装置に送り返す。検証装置は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。レスポンスから逆に秘密情報を求めることを計算量的に困難とすることで、チャレンジとレスポンスを秘密通信とする必要がなくなる。

【００１２】この方法は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか表現できない。また、チケットを証明装置に送信する方法が、第２の従来技術と同様に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できないという問題があった。

【００１３】このように、従来の技術はいずれも、チケットに必要な不正利用を防止する機能を実現するために、第三者に対するチケットの内容証明の機能や利用者の匿名性を犠牲にしている点に、問題があった。

【００１４】［関連技術］これらの問題を解決する関連技術として、特願平９－１８８０６４号（平成９年７月１４日、未公開）に示す方法が提案されている。

【００１５】この関連技術の一般的な認証プロトコルを図１に示す。このプロトコルは、双方向の認証を行うプロトコルであり、双方が認証情報（発生した乱数）に対する署名を確認することによって、お互いの正当性を認証する。相互の認証情報（乱数）の一部にメッセージ（ｍ，μ）を含ませることにより、情報の安全な伝達を可能にしている。

【００１６】図１を参照して関連技術のプロトコルについて説明する。図１において、はじめに、検証装置が乱数に基づいて認証情報Ｃを生成し（Ｓ１１）、この認証情報Ｃを証明装置に対して送る（Ｓ１２）。他方、証明装置は乱数に基づいて別の認証情報χを生成し、認証情報χを検証装置に送る（Ｓ１３、Ｓ１４）。証明装置にはチケットに対応して、外部からは操作不能な内部状態があり、検証装置からの応答情報によってのみ書き換えが可能となっている。検証装置はχの一部に、内部状態の変更を許可する情報（μ）を含ませた応答情報を作成し、検証装置が署名して証明装置に送る（Ｓ１５、Ｓ１６）。証明装置は応答情報ρの署名を確認することにより、送信者が正当な検証装置であることを確認し、それをもって内部状態変更の情報μの正しさを確認する（Ｓ１７）。ρが正しい場合にのみ、証明装置の内部状態がμの内容にしたがって変更される（Ｓ１８）。証明装置は、正当に作成されたチケットｔと証明装置固有情報ｄｕから、Ｄを復元することが可能であり（Ｓ１９）、最後に証明情報ＲにＤによる署名を施して、検証装置に送り（Ｓ２０、Ｓ２１）、検証装置はその署名を確認することにより、定められたサービスを提供する（Ｓ２２、Ｓ２３）。

【００１７】この方法によれば、チケットの検証情報は公開であるため第３者にもチケットの検証が可能であり、利用者はチケットの検証時に利用者を特定する情報を提示する必要が無いことから、匿名性も守られている。

【００１８】また、検証装置と証明装置がそれぞれの秘密情報と公開情報を持ち合い、相互の認証をすることにより、証明装置・検証装置の偽造の問題を解決している。さらに、この証明に用いる認証情報の一部に、伝達したい情報を埋め込むことにより、検証装置・証明装置相互の情報伝達をも可能にしており、チケットの内容を証明することができる。

【００１９】このように、この関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができ、上記の問題をすべて解決することが可能である。

【００２０】ところで、先の関連技術では、検証装置がチケットを特定する情報を証明装置に送ることにより、検証装置が検証しようとするチケットが証明装置の中で一意に定まることを前提としている。しかし、実際には、その検証装置で検証可能なチケットが証明装置内に複数存在することも考えられる。たとえば、鉄道の乗車券のようなものを考えた場合、その駅から有効な回数券や定期券など複数のチケットが証明装置の中に存在することがありうる。そのような場合、証明装置では、どのチケットを利用者が利用しようとしているのか判断することができない。そこで、こういった場合には、利用者

があらかじめ利用するチケットを選択する必要が生ずる。

【００２１】そして、このような場面において、先の関連技術を適用すると、チケットに対応する内部状態の変更を許可する応答情報が、選択・提示されたチケットの内容を確認することなしに作成され、送られてしまうという問題が生ずる。

【００２２】これは、例えば、利用者が誤ったチケットを選択してしまった場合に、意図しないチケットの内部状態が変更されてしまうことを意味している。

【００２３】また、鉄道の切符に適用する場合を考えると、内部状態として、入場の記録を残しておき、出場時に入場の記録を確認することにより、キセルのような不正行為を防止することが考えられる。

【００２４】ここで、入場の情報として、単に入場したという事実のみを、チケットに対応する内部状態に残すような場合を考える。このような場合、内部状態の変更許可情報、具体的には入場情報を、提示されたチケットの内容を確認すること無く証明装置に送ってしまうと、本来その駅では入場できないチケットに対しても、入場したという事実を残すことが可能になる。実際には正当でないチケットでの入場はできないが、入場を拒否された段階で、内部状態が書き換えられたチケットを保持している証明装置を手に入れることができるとすると、実際に入場した駅よりも目的駅に近い駅からのチケットに対する入場記録を偽造すれば、出場時に偽造した入場記録を持つチケットを提示することで、キセル行為が可能になってしまう。

【００２５】このように、利用者が、証明しようとするチケットを自ら選択するような場合には、検証装置は、内部状態を変更する許可情報を作成する前に、提示されたチケットがその検証装置で正当に検証可能であることを確認する必要がある。

【００２６】しかし、先の関連技術においては、このような確認が成されないため、利用者が誤って意図しないチケットに対応する内部状態を書き換えてしまったり、内部状態を書き換えることによる不正が可能であったりするという問題点があった。

【００２７】

【発明が解決しようとする課題】本発明では、上記の問題を解決するために、検証装置が検証可能なチケットのみを検証し、検証することが正しくないチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することを目的とする。

【００２８】

【課題を解決するための手段】上記の課題を解決するため、本発明に係わる電子チケットシステムは、チケット検証装置と証明装置からなり、チケット検証装置は、検証するチケットが検証装置で検証可能かどうかを、証明装置が提示するチケット判定情報に基づいて判定するチケット判定手段と、証明装置がチケット秘密情報を算出できたか否かを検証する対話検証手段を有し、証明装置は、証明装置固有情報保持手段と、チケット保持手段と、少なくとも証明装置固有情報とチケットからチケット秘密情報に関する知識の証明を行える対話証明手段とを有している。

【００２９】この構成においては、検証装置が、チケット判定情報に基づいて、証明装置内のチケットの適合性をチェックでき、正しいチケットが提示されたときのみ証明装置の内部状態を変更するようにできる。

【００３０】

【発明の実施の態様】以下、本発明を詳細に説明する。

【００３１】［実施例１］図２に本発明の実施例１の電子チケットシステムの構成図を示す。図２において、本実施例に示す電子チケットシステムは、検証装置（検証器ともいう）１００と証明装置（証明器ともいう）２００とチケット指定装置３００とからなる。

【００３２】検証装置１００は、検証するチケットの正当性を判定するチケット判定部１０１と、認証情報生成部１０２と、証明情報生成部１０３と、証明情報検証部１０４と、検証装置特権情報保持部１０５と、通信部１０６とを含んで構成される。

【００３３】一方、証明装置２００は、証明装置固有情報保持部２０１と、チケット保持部２０２と、チケット判定情報生成部２０３と、認証情報生成部２０４と、証明情報検証部２０５と、証明情報生成部２０６と、内部状態制御部２０７と、通信部２０８とを含んで構成される。なお検証装置１００の証明情報生成部１０３、認証装置２００の証明情報生成部２０６は、それぞれ認証装置２００、検証装置１００から送られてくる認証情報を保持する記憶部を具備している。

【００３４】また、チケット保持部２０２にはチケットと、各チケットに対応するチケット利用情報とが保存される。また、チケット保持部２０２には各チケットに対応する内部状態記憶領域が確保される。

【００３５】ここでは、証明装置２００は、内部のデータや処理手続きを外部から観測することが困難なＩＣカードのような媒体により構成される。

【００３６】また、この実施例では以下のように、チケットｔが発行される。

【００３７】

【表１】

チケット：ｔ＝Ｄ－Ｆ（ｎ，Ｌ，ｄｕ）

Ｄ：チケット秘密鍵

ｄｕ：証明装置固有の秘密情報

ｎ：チケット法数

Ｆ：非衝突性一方向関数

Ｌ：チケット利用情報

ただし、

ＥＤ≡１ｍｏｄ　ｎ

ここでＥ：チケット公開鍵
である。チケット秘密情報がＤであり、チケット公開情報は、Ｅ，ｎ，Ｌである。Ｆは一般のハッシュ関数によって実現可能である。また、チケット利用情報Ｌには、そのチケットを利用する条件、例えば有効期限や、サービスを受けられる場所などの情報が入る。

【００３８】本発明の認証プロトコルの概略を図３に示す。はじめに利用者は、これから利用するチケットをチケット指定装置３００により証明装置２００に指定した上で、検証装置１００と証明装置２００との間で認証プロトコルが開始される。

【００３９】図３において、認証プロトコルでは、まず検証装置１００の認証情報生成部１０２が、認証情報として乱数Ｃを生成し証明装置２００に送る（Ｓ３１、Ｓ３２）。

【００４０】認証情報を受け取った証明装置２００は、チケット証明情報生成処理を実行する（Ｓ３３）。

【００４１】チケット証明情報生成処理（Ｓ３３）のフローチャートを図４に示す。図４において、まず証明装置２００の証明情報生成部２０６は、署名に用いる秘密鍵Ｄを、チケットｔとチケット利用情報Ｌおよび証明装置固有情報保持部２０１に保存されている証明装置固有情報ｄｕから、以下の計算により算出する（Ｓ４１）。

【００４２】
【数７】
$$t+F(n, L, du)$$
$$=D-F(n, L, du)+F(n, L, du)$$
$$=D$$

次に、チケット判定情報生成部２０３は、正しいチケットを保持していることを示すためのチケット判定情報Ｍを、チケット保持部２０２のチケット利用情報および内部状態記憶領域の情報から生成する（Ｓ４２）。証明情報生成部２０６は、認証情報Ｃのビット列の下位にチケット判定情報Ｍを連結し（Ｓ４３）、チケット証明情報Ｔを、

【００４３】
【数８】$T=(C||M)^{e} \bmod n$
の計算により生成する（Ｓ４４、なお記号｜｜はビット列に連結することを示す）。なお上記の計算以外にも、

【００４４】
【数９】$T=(C||M)'(C||M)^{F(n,L,du)} \bmod n$
により、証明情報Ｔを計算しても良い。

【００４５】また、認証情報生成部２０４は、乱数χを生成し第２の認証情報とする（Ｓ４４）。

【００４６】チケット証明情報Ｔと第２の認証情報χは、通信部２０８により検証装置１００に送られる（Ｓ３４）。署名をするのは、チケット証明情報が正しいものであり、証明装置・チケット判定情報が偽造されていないことを保証するためである。

【００４７】Ｔとχを受け取った検証装置１００はチケット判定処理（図３のＳ３５）を行う。

【００４８】チケット判定処理（図３のＳ３５）のフローチャートを図５に示す。図５において、検証装置１００の証明情報検証部１０４は、送られたチケット証明情報Ｔと証明情報検証部が保持しているチケット公開情報Ｅから、

【００４９】
【数１０】$T^{e} \bmod n$
の値を計算し、そのビット列のうち、連結された上位ビットの部分が、認証情報Ｃと一致するかどうかを確認する（Ｓ５１）。一致した場合には、さらにチケット判定情報Ｍを抽出する（Ｓ５２）。次に、チケット判定部１０１は、Ｍの内容をもとにチケット及びチケットに関連付けられた内部状態がこの検証装置で検証して良いものかどうかを判定する（Ｓ５３）。判定の結果、このチケットを検証して良い場合には、証明情報生成部１０３は、証明装置２００の内部状態の変更を指示する情報μを作成して、χの下位に連結する（Ｓ５４、Ｓ５５）。さらに、この値に対して、検証装置の特権を表す秘密情報δを用いて署名をした値ρを作成する（Ｓ５６）。作成されたρは、通信部１０６により証明装置２００へと送られる（Ｓ３６）。

【００５０】一方、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないものの場合には、プロトコルを終了する（Ｓ５７）。

【００５１】次にρを受け取った証明装置は内部状態変更処理（図３のＳ３７）を行う。

【００５２】内部状態変更処理（図３のＳ３７）のフローチャートを図６に示す。図６において、証明装置２００の証明情報検証部２０５は、送られた第２の証明情報ρに対して、自身が保持している検証装置１００の特権を確認する公開情報εを用いて

【００５３】
【数１１】
$$\rho^{\varepsilon} \bmod \nu$$
を計算し、そのビット列のうち、上位の部分が、第２の認証情報χと一致するかどうかを確認する（Ｓ６１）。確認の結果、正しくないことが判明した場合には場合には、プロトコルを終了する（Ｓ６２）。正しいものであることが確認できた場合には、連結されたμを抽出する（Ｓ６３）。内部状態制御部２０７は、μの内容に応じて証明装置２００の内部状態を変更し、その結果をＭ'とする（Ｓ６４、Ｓ６５）。証明情報生成部２０６はＭ'の値を認証情報Ｃのビット列に連結した上で、

【００５４】
【数１２】$R=(C||M')^{e} \bmod n$
の計算により、証明情報Ｒを生成する（Ｓ６６、Ｓ６７）。Ｒは通信部２０８により検証装置１００に送られる（Ｓ３８）。

15

【００５５】Ｒを受け取った検証装置１００は、証明情報検証処理（図３のＳ３９）を行う。

【００５６】証明情報検証処理（図３のＳ３９）のフローチャートを図７に示す。図７において、検証装置１００の証明情報検証部１０４は保持しているチケット公開情報Ｅを用いて、

【００５７】

【数１３】$R^{e} \bmod n$

の値を計算し、その結果連結されたＭ'を除いた上位のビット列が、最初に検証装置１００が生成した認証情報Ｃと一致することを確認する（Ｓ７１）。確認できた場合は、さらに内部状態の変更結果を表す情報Ｍ'の内容が、第２の証明情報ρとして送った、内部状態変更を許可する情報μと一致するかどうかを確認し（Ｓ７２、Ｓ７３、Ｓ７４）、確認ができた場合には、定められたサービスを提供する（Ｓ７５）。いずれかの確認に失敗した場合には、プロトコルが終了し、サービスの提供は行われない（Ｓ７１、Ｓ７４、Ｓ７６）。

【００５８】［実施例２］本発明の実施例２は、実施例１を鉄道の切符の乗車券として実現した場合である。ここでは特に、乗車券の入場時のプロトコルを説明する。

【００５９】本発明の実施例の構成やチケットの生成方法は実施例１と同様であるが、検証装置１００は具体的には自動改札機であり、証明装置２００はチケットを保持することができる、ＩＣカードのようなトークンである。そして、入場、出場ともに自動改札による検証が行われ、内部状態には入場や出場に対応した記憶領域が確保されるものとする。

【００６０】以下では、横浜～成田空港１９９７年７月１８日の乗車券の例で説明する。なお、適宜、図３の対応するステップ等を指摘する。

【００６１】チケットのチケット利用情報Ｌは、図９のようになる。チケットは証明装置２００に登録されており、対応した内部状態記憶領域が確保されている。入場前の内部状態を図８に示す。ここで、これから使用するチケットは、チケットＩＤが００００５に示すものである。

【００６２】まず、入場時の認証について説明する。はじめに検証装置１００は認証情報Ｃとともに、入場であることをあらわす情報を証明装置２００に送る（Ｓ３２）。

【００６３】証明装置２００は、チケット判定情報Ｍを生成する。Ｍの内容を図１０に示す。チケット判定情報Ｍには、図に示すように、チケット利用情報に含まれる内容と、使用状態を示すための、内部状態の入場・出場記録の内容が含まれている。証明情報生成部２０６は、ＭをＣに連結し、チケット秘密鍵Ｄによる署名を施して、チケット証明情報Ｔとして、生成した第２の認証情報χとともに検証装置１００に送る（Ｓ３４）。

【００６４】検証装置１００は、チケット証明情報を検証し、さらにチケット判定情報Ｍの内容を確認する。ここでは、入場駅が横浜駅で、有効期限内であり、未使用のチケットであることから、ここでの認証をしてよいチケットであると判定される（Ｓ３５）。

16

【００６５】そこで、証明装置２００の内部状態を変更するための情報μが作成される。μの内容を図１１に示す。μには、入場駅名と時間が記録される。証明情報生成部１０３は、こうして生成したμを第２の認証情報χに連結し、検証装置１００の特権情報δによる署名を施した値ρを生成して、証明装置２００へ送る（Ｓ３６）。

【００６６】証明装置２００の証明情報検証部２０５は、送られたρの値が、認証情報χと一致するかどうかを確認する。正しいものであることが確認できた場合には、内部状態制御部２０７がμの内容に応じて、証明装置２００の内部状態を変更する（Ｓ３７）。変更後の内部状態の様子を図１２に示す。入場の駅と時間が記録されたことがわかる。次に、内部状態制御部207はこの内部状態の変更、すなわち入場記録の内容をＭ'とする。実施例１と同様に、証明情報生成部２０６は、Ｍ'の値を認証情報のビット列に連結して、チケット秘密情報による署名を施した値Ｒを生成して、証明情報Ｒとして検証装置１００に送る（Ｓ３８）。

【００６７】検証装置１００は証明情報Ｒの値を検証し、その値が認証情報Ｃと一致した場合には、さらに内部状態を変更した結果Ｍ'を確認する。Ｍ'がμで指定したものと対応していれば、正しく内部状態が変更されたものと判断し、改札機のゲートを開ける。

【００６８】次に、出場時の認証を説明する。出場時の認証は、入場時とほぼ同様であるが、相互に伝えられるメッセージの内容が異なる。

【００６９】はじめに検証装置１００は認証情報Ｃとともに、出場であることをあらわす情報を証明装置に送る（Ｓ３２）。

【００７０】証明装置２００のチケット判定情報生成部２０３はチケット判定情報Ｍを生成する。出場時のＭの内容を図１３に示す。証明情報生成部２０６は、ＭをＣに連結し、チケット秘密鍵Ｄによる署名を施し、チケット証明情報Ｔとする。そして、証明情報Ｔと、認証情報生成部生成した第２の認証情報χが検証装置に送られる（Ｓ３４）。

【００７１】検証装置１００の証明情報検証部１０４は、チケット証明情報を検証する。チケットの検証結果か正しい場合には、チケット判定部１０１が、チケット判定情報Ｍの内容を確認する。ここでは、入場駅が横浜駅で有効な入場記録であり、出場の有効期間内であることから、ここでの出場の認証が可能なチケットであると判定される（Ｓ３５）。

【００７２】次に、証明情報生成部１０３は証明装置２００の内部状態を変更するための情報μを作成する。μ

の内容を図１４に示す。μには、出場駅名と出場時間が記録される。証明情報生成部１０３は、さらに、生成されたμをχに連結し、検証装置の特権情報δによる署名を施した値ρを生成する。ρは証明装置２００へと送られる（Ｓ３６）。

【００７３】証明装置２００の証明情報検証部２０５は、送られたρの値が、認証情報χと一致するかどうかを確認する。正しいことが確認できた場合には、内部状態制御部２０７がμの内容に応じて、証明装置２００の内部状態を変更し、この変更結果、すなわち出場記録をM'とする。変更後の内部状態の様子を図１５に示す。出場駅と時間が記録される。証明情報生成部２０６は、出場記録M'を認証情報Ｃのビット列に連結して、チケット秘密情報による署名を施した証明情報Ｒを生成し、検証装置１００に送る（Ｓ３８）。

【００７４】検証装置２００の証明情報検証部１０４はＲの値を検証し、その値が認証情報Ｃと一致した場合には、さらに内部状態を変更した結果M'を確認する。M'がμの値で指定したものと対応していれば、正しく内部状態が変更されたものと判断し、出場を許可して、改札機のゲートを開ける（Ｓ３９）。

【００７５】［実施例３］実施例３では、回数券のような形態を実現する方法を示す。

【００７６】基本的には本実施例の構成やチケットの生成方法、全体の処理の流れは実施例１と同様である。本実施例の全体の構成を図１６に示す。本実施例の特徴として、内部状態の中に、回数券の残り度数を示すカウンタ２０２ａが設置されている点が異なる。図１６においては、図２と対応する箇所に対応する符号を付した。

【００７７】利用者は回数券を購入すると、はじめに証明装置２００に登録する。登録時に回数券に対応する内部状態記憶領域が確保され、そのなかのカウンタ２０２ａに、残りの使用回数が書き込まれる。

【００７８】回数券の利用時には利用者は、証明装置２００に対してこれから利用するチケットとして、チケット指定装置３００により、回数券を指定した上で、検証装置１００と証明装置２００との間で認証プロトコルが開始される。

【００７９】認証プロトコルでは、検証装置１００が、認証情報として乱数Ｃを生成し証明装置２００に送り、証明装置２００が、チケット秘密鍵を計算するところまでは、実施例１と同様である。

【００８０】本実施例のチケット証明情報生成処理（図３のＳ３３に対応）のフローチャートを図１７に示す。図１７において、証明装置２００のチケット判定情報生成部２０３は、この回数券のチケットに対応した内部状態の残り回数を抽出し、チケット利用情報とともに、チケット判定情報Ｍに記録する（Ｓ８１～Ｓ８４）。そして、実施例１と同様に、証明情報生成部２０６がチケット証明情報Ｔを生成し（Ｓ８５）、認証情報生成部２０４が第２の認証情報χを生成する（Ｓ８６）。Ｔとχは通信部２０８により検証装置１００に送られる（Ｓ３４）。

【００８１】Ｔとχを受け取った検証装置１００はチケット判定処理（図３のＳ３５に対応す）を行う。

【００８２】チケット判定処理のフローチャートを図１８に示す。図１８において、検証装置１００の証明情報検証部１０４は、受け取ったチケット証明情報を検証する（Ｓ９１）。チケット証明情報が正しい場合には、チケット証明情報から、チケット判定情報Ｍを抽出する（Ｓ９２）。チケット判定情報Ｍには回数券の残り回数が記録されている。チケット判定部１０１はその値が１以上であれば、この回数券はまだ使用可能であると判断する（Ｓ９３）。さらに、チケット利用情報Ｌの内容も、この検証装置１００で検証可能であるとチケット判定部１０１が判断した場合には、証明情報生成部１０３は証明装置２００の内部状態の変更を指示する情報μを作成する（Ｓ９４、Ｓ９５）。μの内容として、回数券の使用回数を１減らすことを指示する内容が含まれる。そして、実施例１と同様の方法で、μを使用して第２の証明情報ρを作成し（Ｓ９６、Ｓ９７）、証明装置２００へと送る（Ｓ３６）。

【００８３】検証やチケット判定に失敗したときにはエラー処理を行なう（Ｓ９８）。

【００８４】ρを受け取った証明装置２００は内部状態変更処理（図３のＳ３７に対応）を行う。

【００８５】内部状態変更処理のフローチャートを図１９に示す。図１９において、証明装置２００の証明情報検証部２０５は送られた第２の証明情報ρを検証する（Ｓ１０１）。正しいものであることが確認できた場合には、内部状態制御部がμの内容に応じて、回数券の残り使用回数を１減らし、その結果をM'とする（Ｓ１０２～Ｓ１０４）。あとは、実施例１と同様の方法で、証明装置２００は証明情報Ｒを生成して、検証装置１００に送る（Ｓ１０５、Ｓ１０６）。ステップＳ１０１で検証に失敗したときにはエラー処理が行なわれる（Ｓ１０７）。

【００８６】以降の検証装置１００の動作は、実施例１と同様であり、Ｒの値を検証して、サービスの提供を行う。

【００８７】［実施例４］本発明の実施例４では、全体の構成は実施例１と同様であるが、チケット公開情報・チケット秘密情報やチケットの認証方法が異なる。

【００８８】本実施例では、ｐが素数であり、Ｇが離散対数問題が困難な有限群であり、ｇが有限群Ｇの位数ｐの元であり、

【００８９】

【数１４】$y = g^{x} \bmod p$

が満たされるとき、（ｐ，Ｇ，ｇ，ｙ）がチケット公開情報であり、ｘをチケット秘密情報とする。（ｐ，Ｇ，

19

ｇ）はシステム全体で共通とすることもできる。

【００９０】このとき、チケットはチケット特徴情報ｘと証明装置固有情報ｄｕとチケット利用情報Ｌと、群を規定する情報ｐより、

【００９１】

【数１５】ｔ＝ｘ－Ｆ（ｄｕ，Ｌ，ｙ，ｐ）

として、計算される。ここで、Ｆは非衝突性の一方向関数であり、一般のハッシュ関数によって実現可能である。Ｌは実施例１と同様のチケット利用情報である。

【００９２】また、検証装置の特権をあらわすものとして、上記（ｐ，Ｇ，ｇ）は共通として、

【００９３】

【数１６】

$$\eta = g^{\xi} \mod p$$

を満たすようなηを公開情報、ξを秘密情報とする。

【００９４】実際にはＧを乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【００９５】本発明の認証プロトコルの概略を図２０に示す。

20

【００９６】はじめに利用者は、これから利用するチケットを証明装置に対して指定した上で、検証装置と証明装置の間で認証プロトコルが開始される。

【００９７】図２０において、この認証プロトコルでは、まず検証装置１００の認証情報生成部１０２が、乱数ｒを生成し、Ｃ＝ｇ'を計算して、これを認証情報として証明装置に送る（Ｓ２０１、Ｓ２０２、Ｓ２０３）。

【００９８】認証情報Ｃを受け取った証明装置２００は、チケット証明情報生成処理を実行する（Ｓ２０４）。

【００９９】チケット証明情報生成処理のフローチャートを図２１に示す。図２１において、まず証明装置２００の証明情報生成部２０６は、署名に用いる秘密鍵ｘを、チケットｔとチケット利用情報Ｌ、チケット公開情報のｐ、および証明装置固有情報ｄｕから、以下の計算により算出する（Ｓ２１１）。

【０１００】

【数１７】

$$\begin{aligned} & t + F(y, L, du, p) \\ &= x - F(y, L, du, p) + F(y, L, du, p) \\ &= x \end{aligned}$$

次に、チケット判定情報生成部２０３は、正しいチケットを保持していることを示すためのチケット判定情報Ｍを、チケットの付加情報Ｌや内部状態の情報から生成する（Ｓ２１２）。証明情報生成部２０６は、証明情報として、以下の値を生成する（Ｓ２１３、Ｓ２１４）。

【０１０１】

【数１８】$T = (C \| M) \cdot C' \mod p$

なお証明情報Ｔは上記以外にも、以下の式によっても計算できる。

【０１０２】

【数１９】

$$T = (C \| M) \cdot C'^{C^{r}(y, L, du, p)} \mod p$$

また、認証情報生成部２０４は同時に乱数ｒ'を生成して、

【０１０３】

【数２０】$\chi = g' \mod p$

を第２の認証情報として検証装置に送る（Ｓ２１５、Ｓ２１６、Ｓ２０５）。チケット判定情報Ｍに入る情報は実施例１～３と同様である。

【０１０４】証明情報Ｔと第２の認証情報χは、通信部２０８により検証装置１００に送られる。

【０１０５】Ｔとχを受け取った検証装置１００はチケット判定処理（図２０のＳ２０６）を行う。

【０１０６】チケット判定処理のフローチャートを図２２に示す。図２２において、検証装置１００の証明情報検証部１０３は、送られたチケット証明情報から、

【０１０７】

【数２１】$T / y' \mod p = (C \| M) \cdot C' /$

$y' \mod p$

の値を計算し、そのビット列のうち、連結されたＭ以外の部分が、認証情報Ｃと一致するかどうかを確認する（Ｓ２２１）。一致した場合には、チケット判定部１０１はさらにチケット判定情報Ｍの内容から、チケット及びチケットに関連付けられた内部状態がこの検証装置１００で検証して良いものかどうかを判定する（Ｓ２２２、Ｓ２２３）。判定の結果、このチケットを検証して良い場合には、証明情報生成部１０３は証明装置２００の内部状態の変更を指示する情報μを作成して、χに連結する（Ｓ２２４、Ｓ２２５）。そして、この値に対して、検証装置の特権を表す秘密情報ξを用いて以下の値を第２の認証情報として、生成する（Ｓ２２６）。

【０１０８】

【数２２】

$$\rho = (\chi \| \mu) \cdot \chi^{\xi} \mod p$$

ρは通信部１０６により証明装置２００へと送られる。一方、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないものの場合には、プロトコルを終了する（Ｓ２２７）。

【０１０９】次にρを受け取った証明装置２００は内部状態変更処理（図２０のＳ２０８）を行う。

【０１１０】内部状態変更処理のフローチャートを図２３に示す。図２３において、証明装置２００の証明情報検証部２０５は、送られた応答情報から、

【０１１１】

【数２３】

$$\rho / \eta^{r'} \overset{21}{\bmod} p = (\chi \| \mu) \cdot \chi^{E} / \eta^{r'} \overset{22}{\bmod} p$$

の値を計算し、そのビット列のうち、連結されたμ以外の部分が、第２の認証情報χと一致するかどうかを確認する（Ｓ２３１）。正しいものであることが確認できた場合には、内部状態制御部２０７が、μの内部状態の変更を指示する情報に応じて、証明装置２００の内部状態が変更し、その結果をM'とする（Ｓ２３２～Ｓ２３４）。一方、確認の結果、正しくないことが判明した場合には場合には、プロトコルを終了する（Ｓ１３７）。

【０１１２】証明情報生成部２０６は、M'の値を認証情報Ｃのビット列に連結した上で、以下の値を証明情報をとして生成する（Ｓ２３５、Ｓ２３６）。

【０１１３】

【数２４】$R = (C \| M') \cdot C' \bmod p$

こうして生成された証明情報Ｒが通信部２０８により検証装置１００に送られる（Ｓ２０９）。

【０１１４】Ｒを受け取った検証装置１００は、証明情報検証処理Ｓ２１０（図２０）を行う。

【０１１５】証明情報検証処理のフローチャートを図２４に示す。図２４において、証明情報検証部１０４は、送られたチケット証明情報から、

【０１１６】

【数２５】$R / y' \bmod p = (C \| M') \cdot C' / y'^{r} \bmod p$

の値を計算し、その結果M'を除いた上位のビット列が、最初に検証装置１００が生成した認証情報Ｃと一致することを確認する（Ｓ２４１）。確認できた場合は、さらに内部状態の変更結果を表す情報M'の内容が、第２の証明情報ρとして送った、内部状態変更を許可する情報μと一致するかどうかを確認し（Ｓ２４２、Ｓ２４３、Ｓ２４４）、確認ができた場合には、定められたサービスを提供する（Ｓ２４５）。いずれかの確認に失敗した場合には、プロトコルが終了し、サービスの提供は行われない（Ｓ２４６）。

【０１１７】

【発明の効果】以上で説明したように、本発明によれば、検証装置が検証可能なチケットのみを検証し、検証することが正しくないチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することができ、利用者の意図しない内部状態の変更や、内部状態の変更による不正行為を防止することができる。

【図面の簡単な説明】

【図１】　関連技術の処理を説明するフローチャートである。

【図２】　実施例１、２、４の構成を全体として示すブロック図である。

【図３】　実施例１の処理全体を説明するフローチャートである。

【図４】　実施例１の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図５】　実施例１の検証装置のチケット判定処理を説明するフローチャートである。

【図６】　実施例１の証明装置の内部状態変更処理を説明するフローチャートである。

【図７】　実施例１の検証装置の証明情報検証処理を説明するフローチャートである。

【図８】　実施例２のトークンの初期の内部状態を示す図である。

【図９】　チケット付加情報の項目を示す図である。

【図１０】　入場時にトークンから改札機に送られるチケット判定情報Ｍを示す図である。

【図１１】　入場時に改札機からトークンに送られる項目μを示す図である。

【図１２】　入場後のトークンの内部状態を示す図である。

【図１３】　出場時にトークンから改札機に送られるチケット判定情報Ｍを示す図である。

【図１４】　出場時に改札機からトークンに送られる情報μを示す図である。

【図１５】　出場後のトークンの内部状態を示す図である。

【図１６】　実施例３の構成を全体として示すブロック図である。

【図１７】　実施例３の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図１８】　実施例３の検証装置のチケット判定処理を説明するフローチャートである。

【図１９】　実施例３の証明装置の内部状態変更処理を説明するフローチャートである。

【図２０】　実施例４の処理を全体として示すフローチャートである。

【図２１】　実施例４の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図２２】　実施例４の検証装置のチケット判定処理を説明するフローチャートである。

【図２３】　実施例４の証明装置の内部状態更新処理を説明するフローチャートである。

【図２４】　実施例４の検証装置の証明情報検証処理を説明するフローチャートである。

【符号の説明】

１００　検証装置
１０１　チケット判定部
１０２　認証情報生成部
１０３　証明情報生成部
１０４　証明情報検証部
２００　証明装置
２０１　証明装置固有情報保持部
２０２　チケット保持部

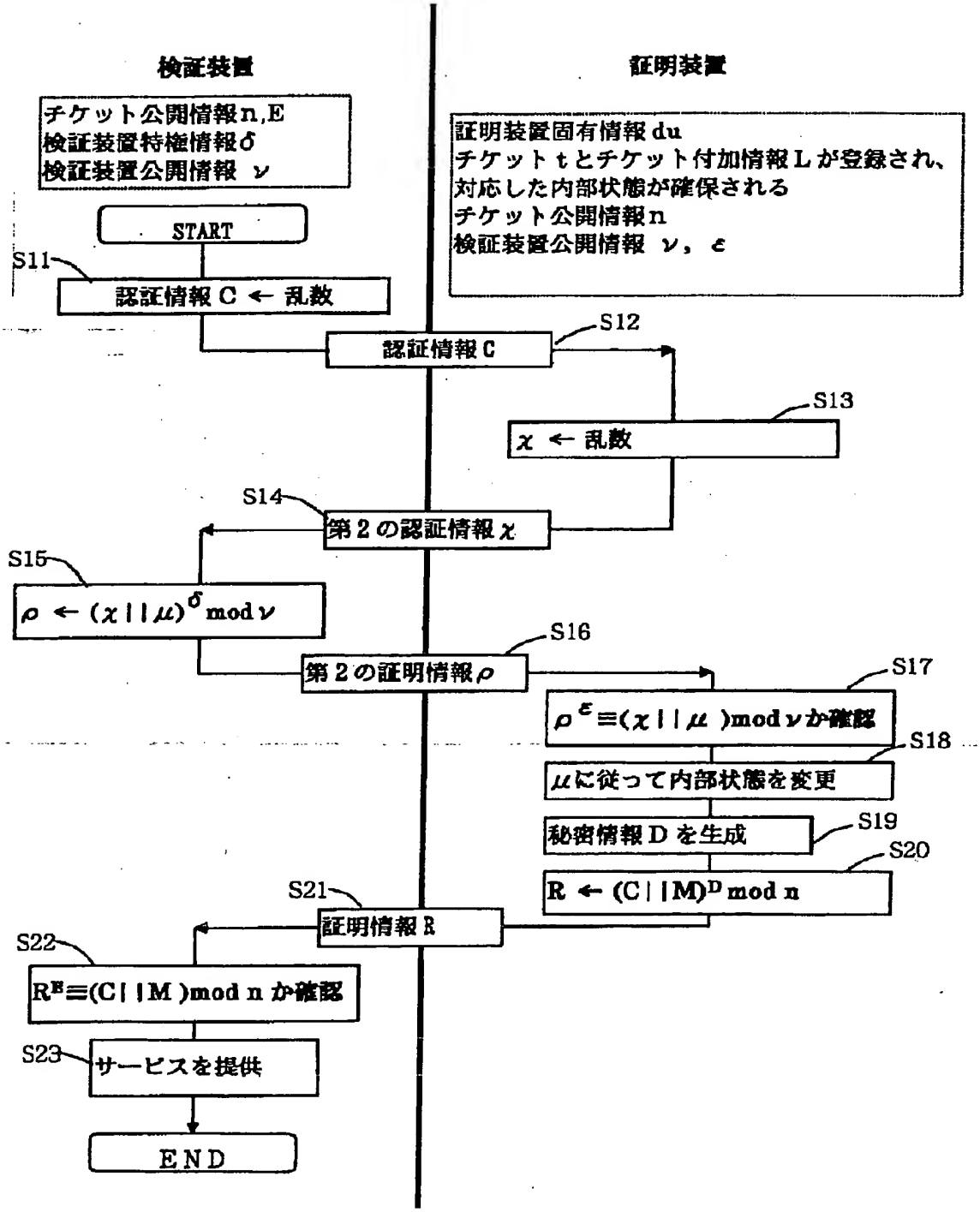
23

２０２ａ　カウンタ
２０３　チケット判定情報生成部
２０４　認証情報生成部
２０５　証明情報検証部

24

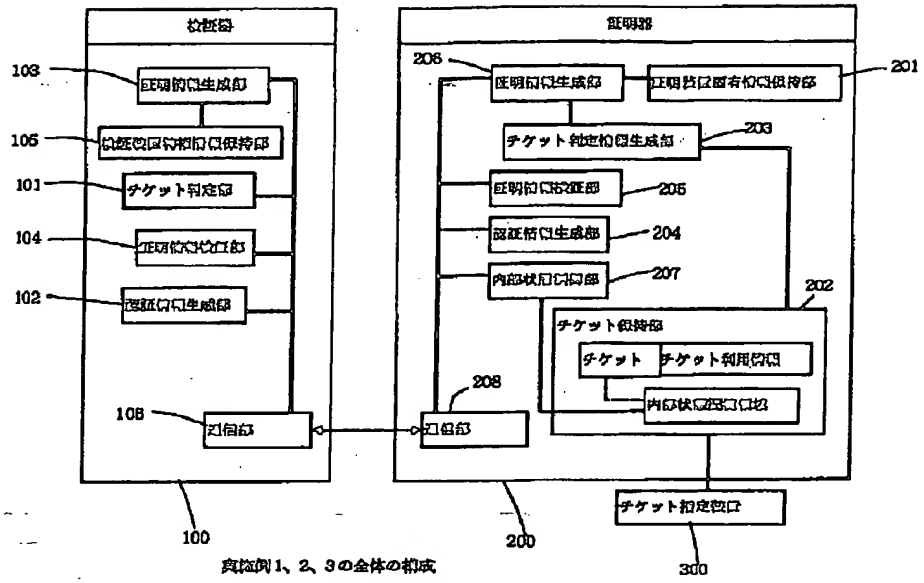
２０６　証明情報生成部
２０７　内部状態制御部
３００　チケット指定装置

【図１】



関連技術の処理のフローチャート

【図２】



実施例1、2、3の全体の構成

【図８】

トークンの内部の内容例

チケットID	発行情報	料金形態	改定履歴	入場情報	出場情報	改札履歴
00001	97/6/31	現金	なし	なし	なし	なし
00003	97/6/31	クレジットカード	なし	97/6/31,9:05 品川	97/6/31,9:30 平塚	なし
00005	97/7/10	現金	なし	なし	なし	なし

【図１０】

入場時にトークンから改札機に送られるチケット判定処理に必要な情報

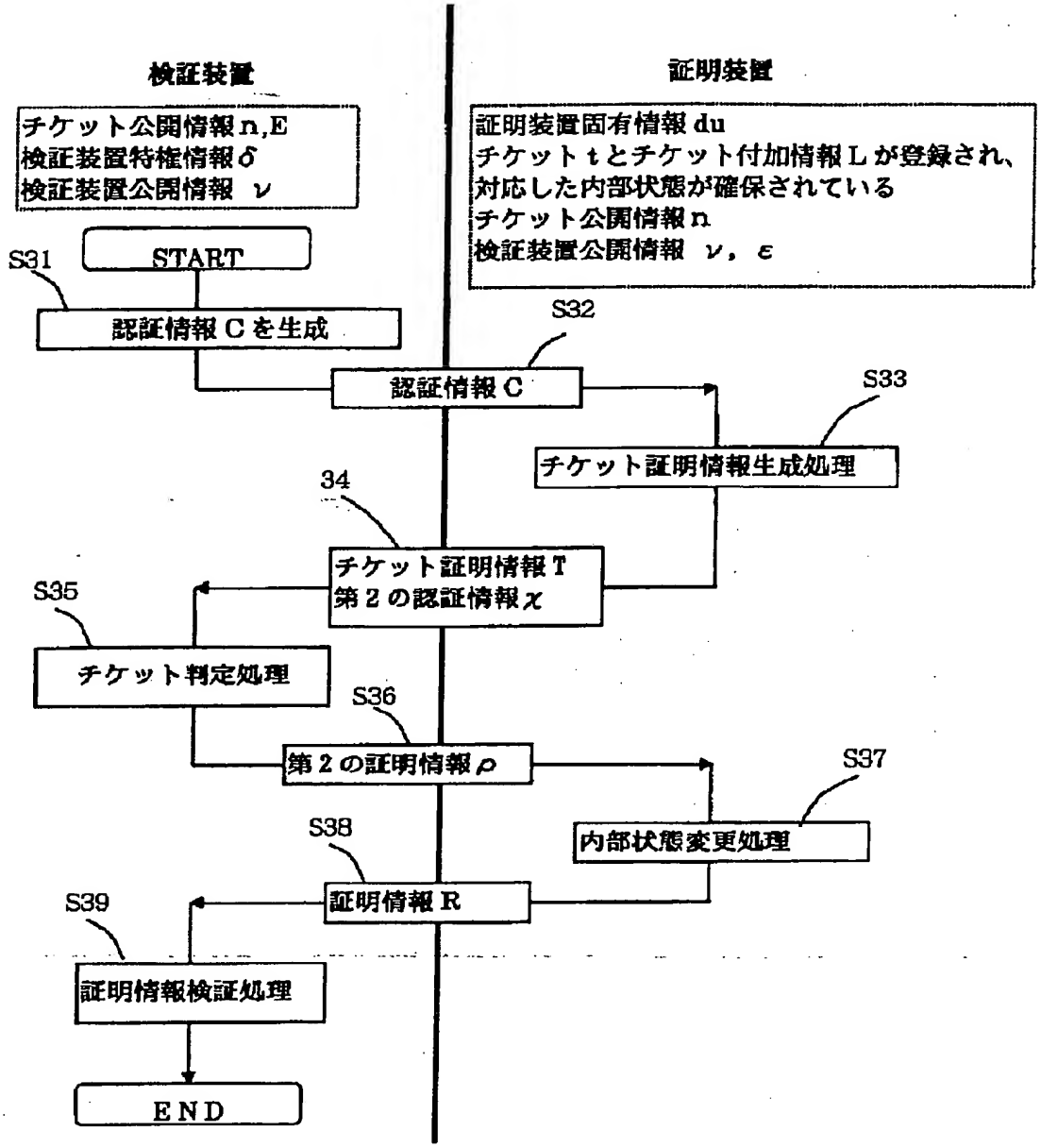
出発駅	目的駅	使用開始日	有効期間	運賃	入場履歴	出場履歴	改札履歴
横浜	成田空港	97/7/18	1日	1000円	なし	なし	なし

【図９】

チケット利用情報の項目

発行ID	発券場所	料金形態	出発駅	目的駅	発行日時	使用開始日	有効期間	運賃
00123	平塚	現金	横浜	成田空港	97/7/10	97/7/18	1日	1000円

【図３】



実施例１の処理全体のフローチャート

【図１１】

入場時に改札機からトークンに送られる項目μ（横浜駅で入場）

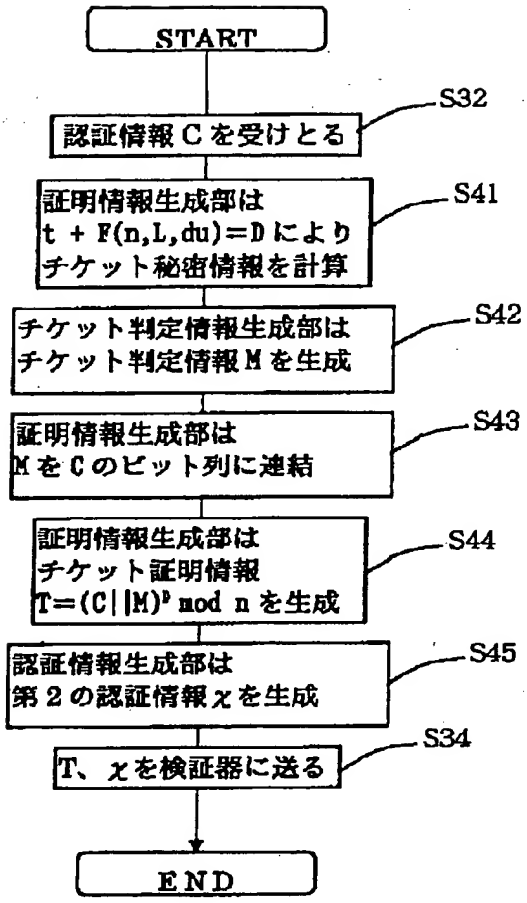
入場駅	入場時間
横浜	97/7/18,8:20

【図１２】

入場後のトークンの内部状態

チケットID	発券情報	料金形態	変更記録	入場記録	出場記録	改札記録
00001	97/6/31	現金	なし	なし	なし	なし
00003	97/6/31	クレジットカード	なし	97/6/31,9:05 横浜	97/6/31,9:20 平塚	なし
00005	97/7/10	現金	なし	97/7/18,6:20 横浜	なし	なし

【図４】



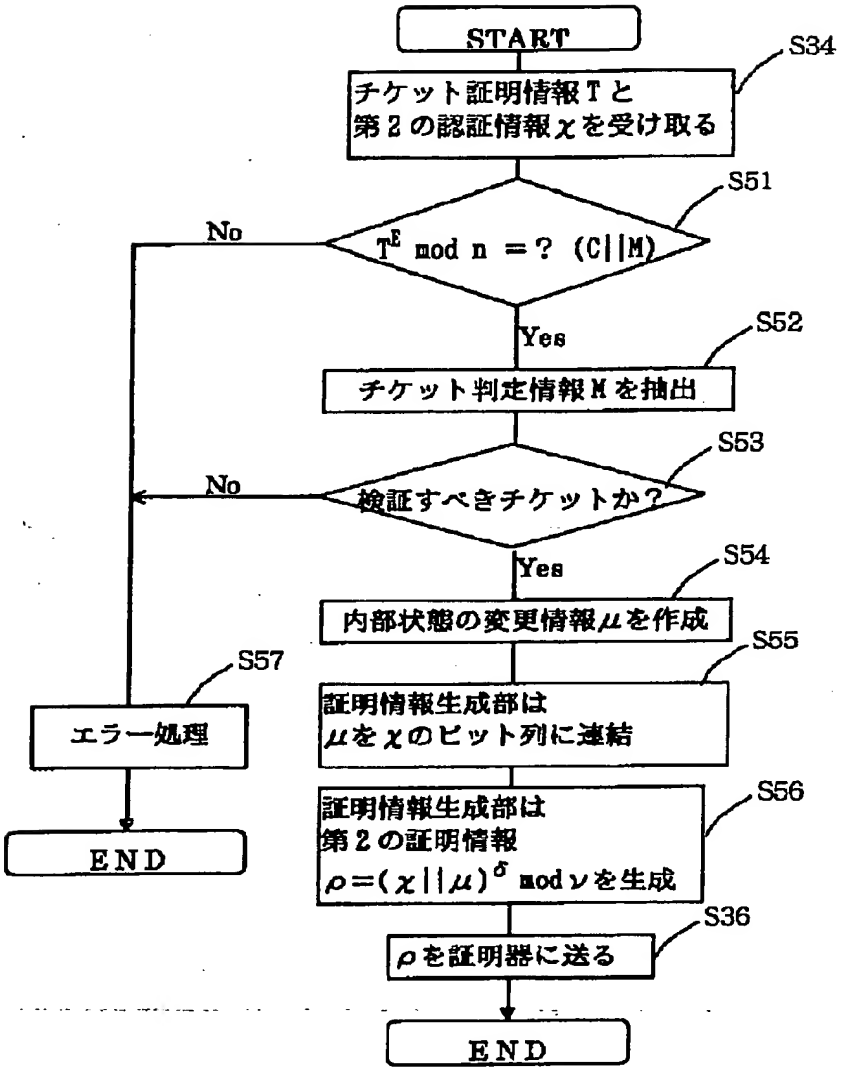
実施例１の証明装置のチケット証明情報生成処理のフローチャート

【図１３】

出場時にトークンから改札機に送られるチケット判定情報 M

出発駅	目的駅	使用開始日	有効期間	経路	入場記録	出場記録	検札記録
横浜	成田空港	97/7/18	1日	東京	97/7/18,6:20 横浜	なし	なし

【図５】



実施例１の検証装置のチケット判定処理のフローチャート

【図１４】

出場駅	出場時間
成田空港	97/7/18,8:53

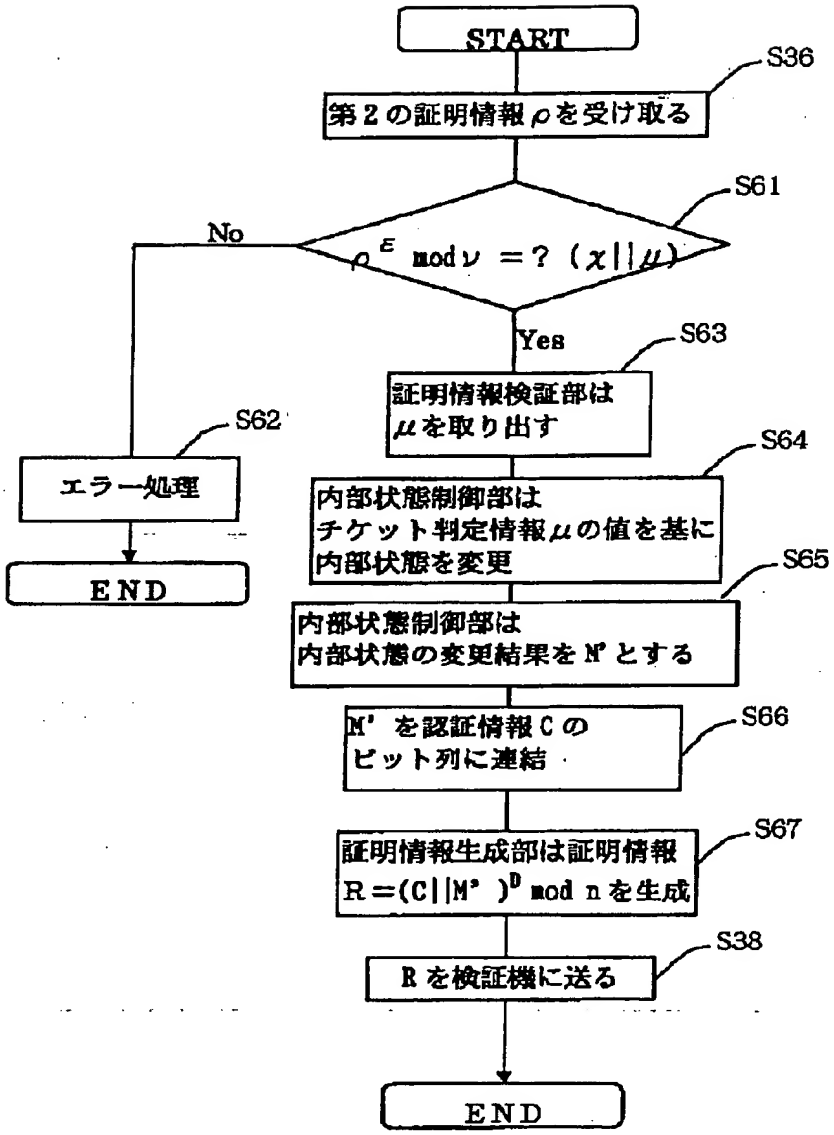
出場時に改札機からトークンに送られる情報 μ(成田空港駅で出場)

【図１５】

出場後のトークンの内部状態

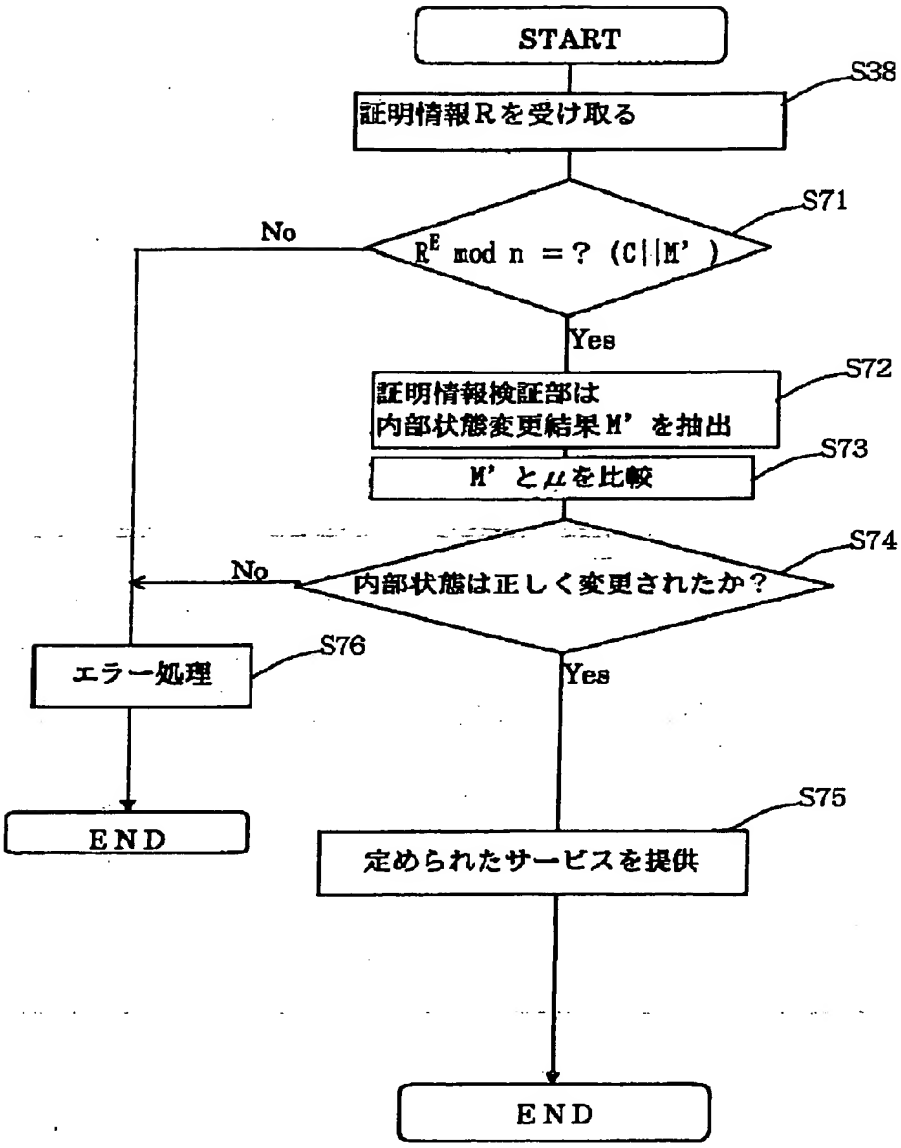
チケットID	発券情報	課金形態	変更記録	入場記録	出場記録	検札記録
00001	97/6/31	現金	なし	なし	なし	なし
00003	97/6/31	クレジットカード	なし	97/6/31,9:05 横浜	97/6/31,9:20 平塚	なし
00005	97/7/10	現金	なし	97/7/18,6:20 横浜	97/7/18,8:53 成田空港	なし

【図６】



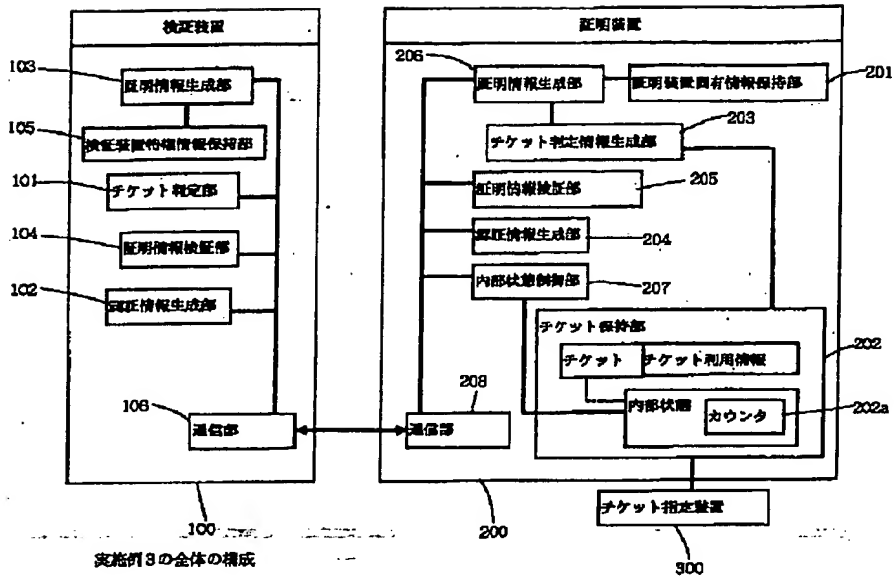
実施例１の証明装置の内部状態変更処理のフローチャート

【図７】



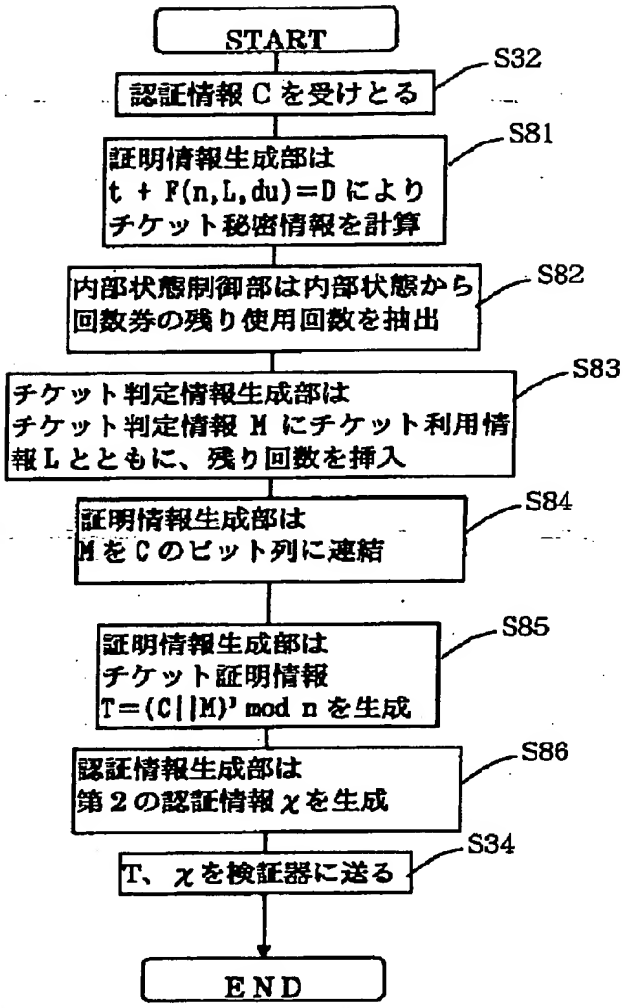
実施例１の検証装置の証明情報検証処理のフローチャート

【図１６】



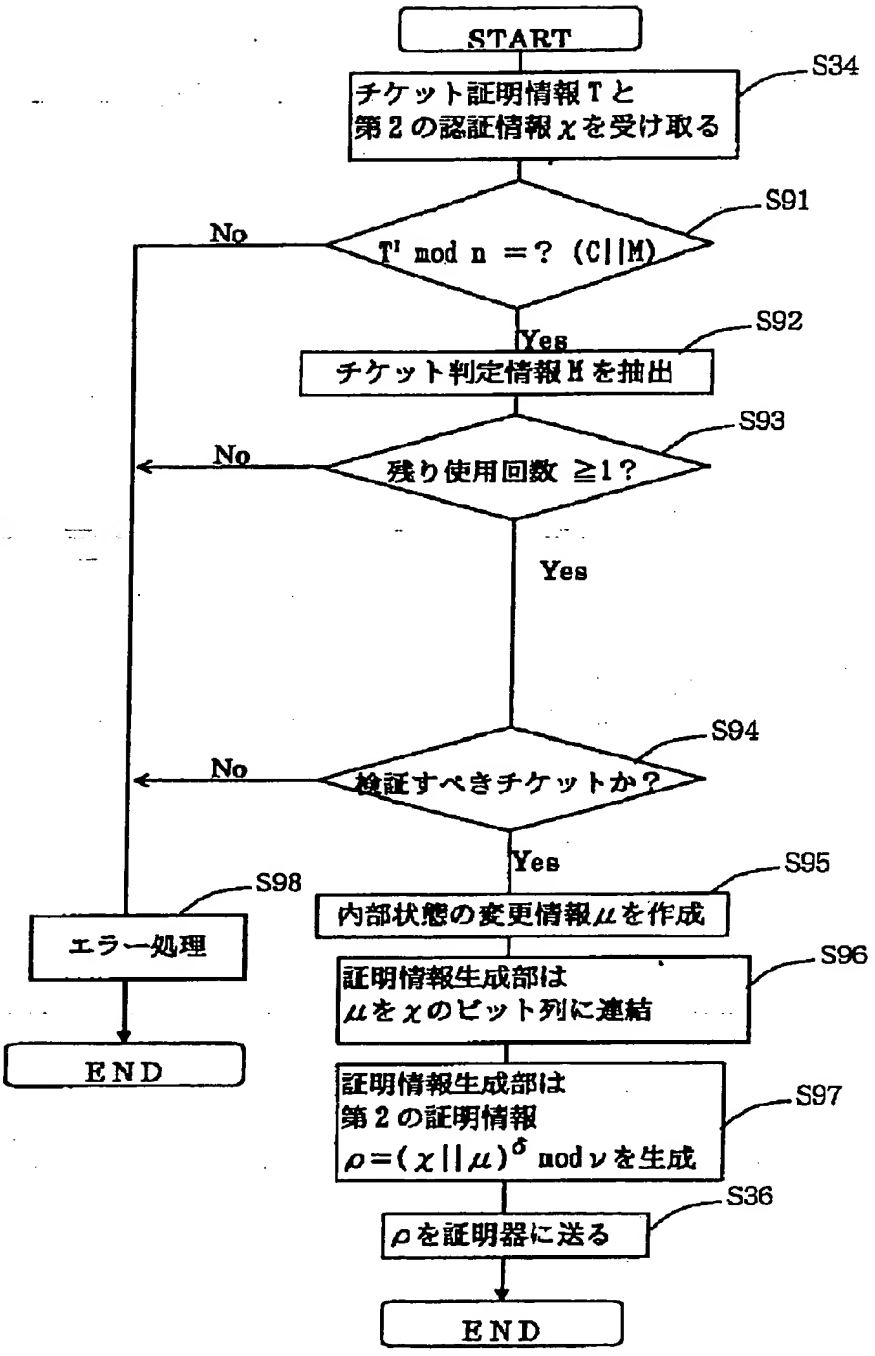
実施例３の全体の構成

【図１７】



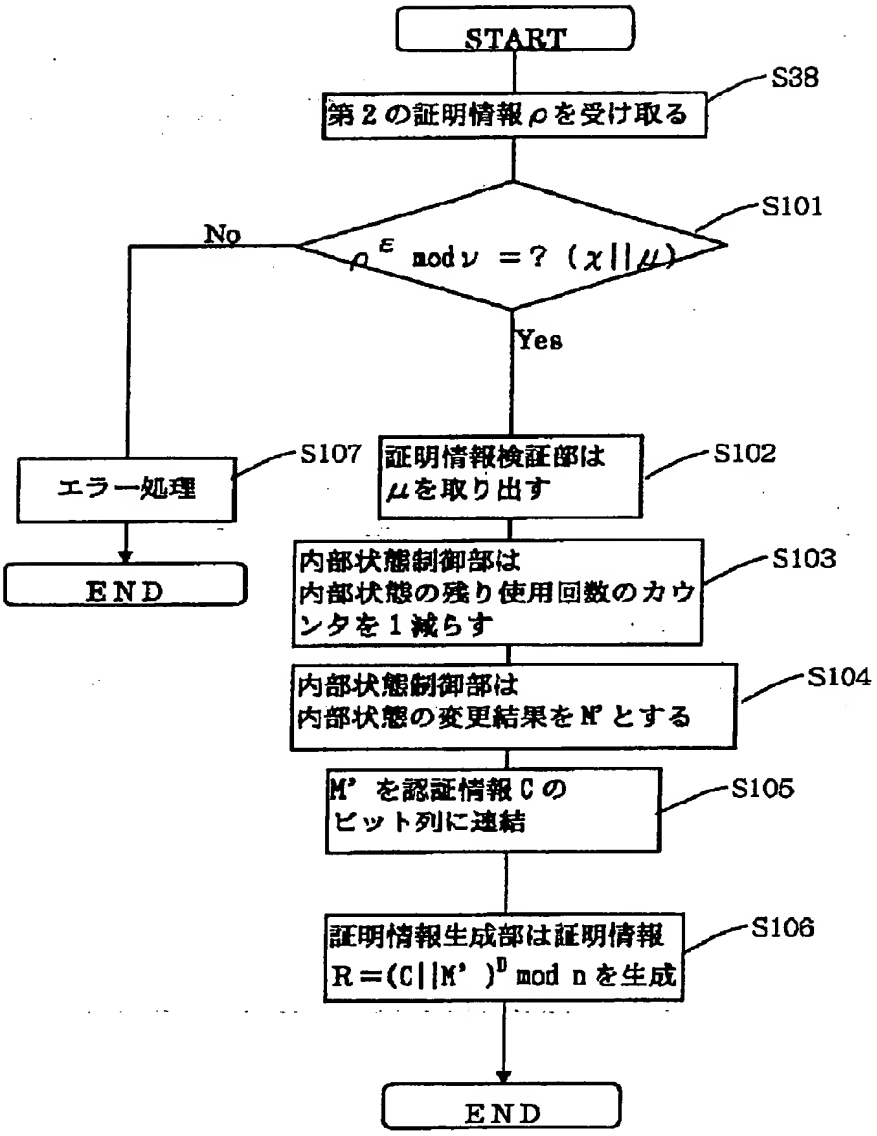
実施例３の証明装置のチケット証明情報生成処理のフローチャート

【図１８】



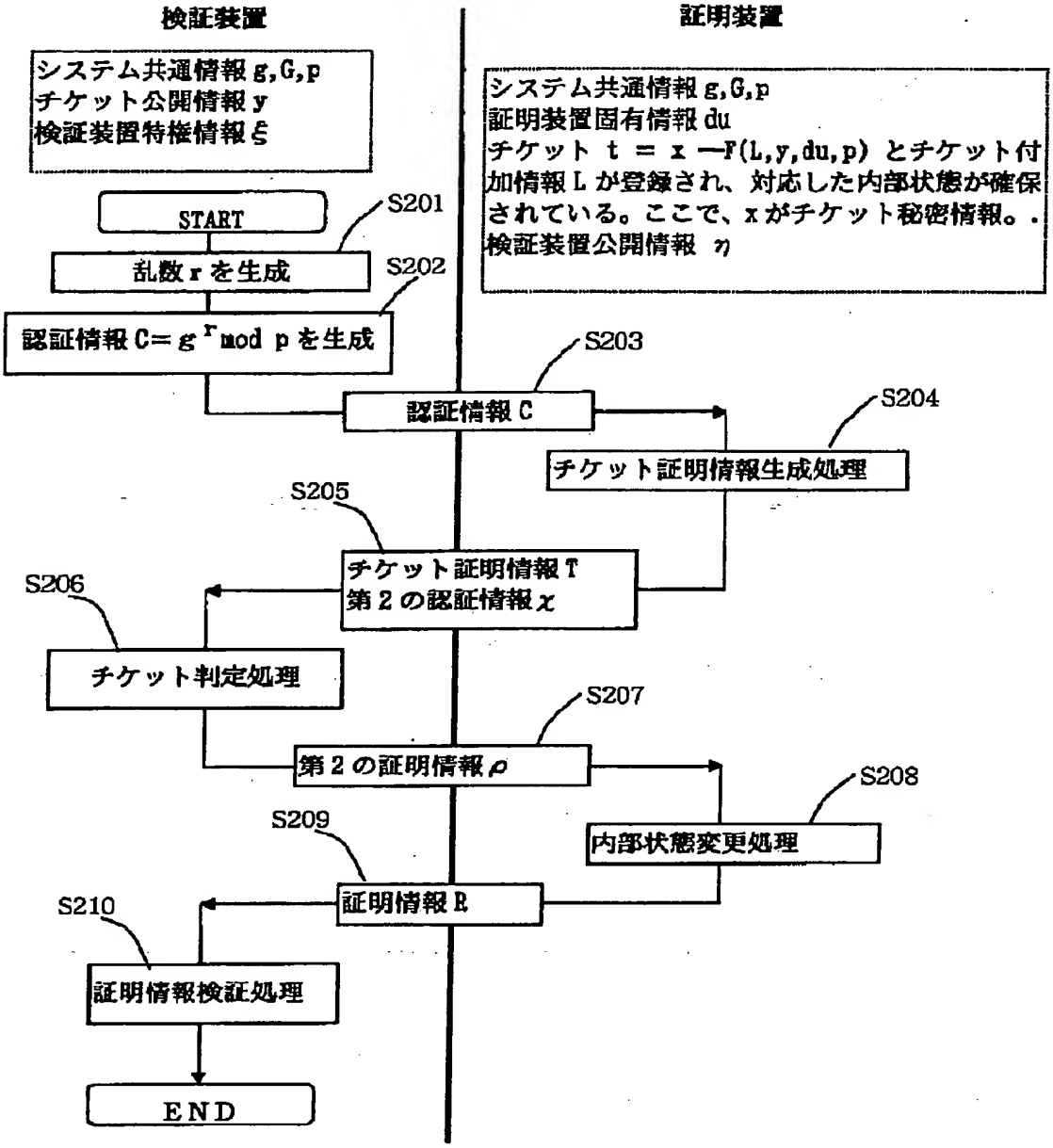
実施例３の検証装置のチケット判定処理のフローチャート

【図１９】



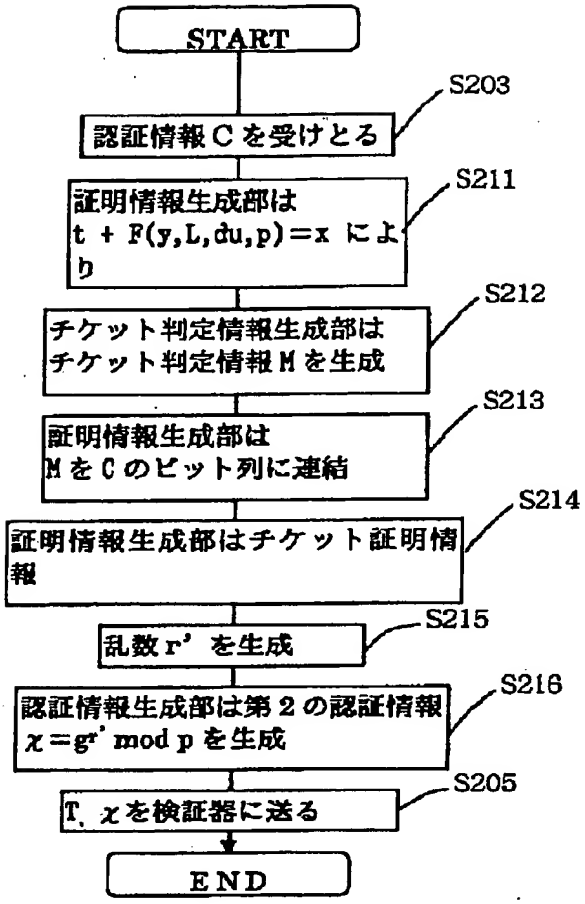
実施例３の証明装置の内部状態変更処理のフローチャート

【図２０】



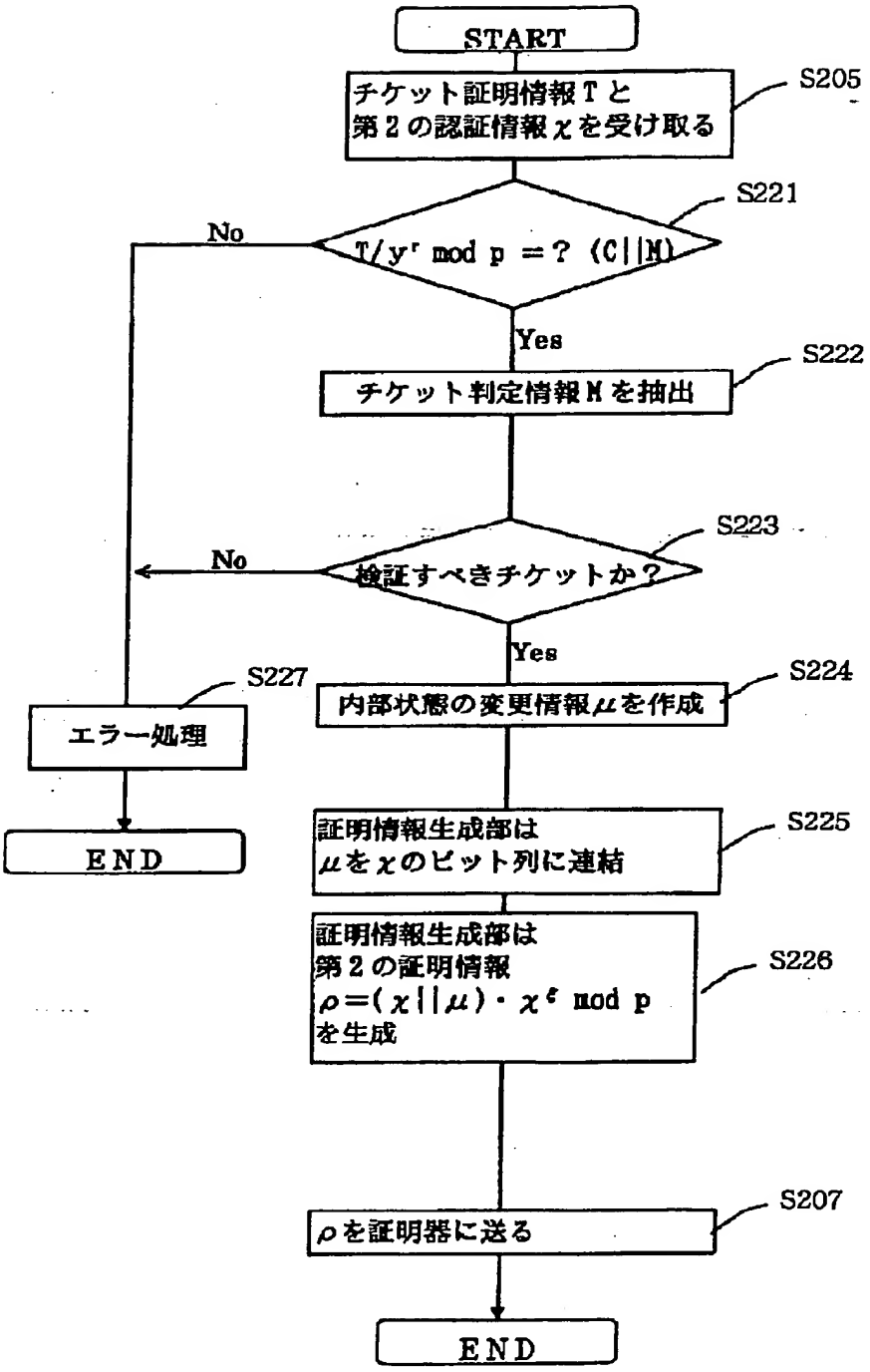
実施例４の処理全体のフローチャート

【図２１】



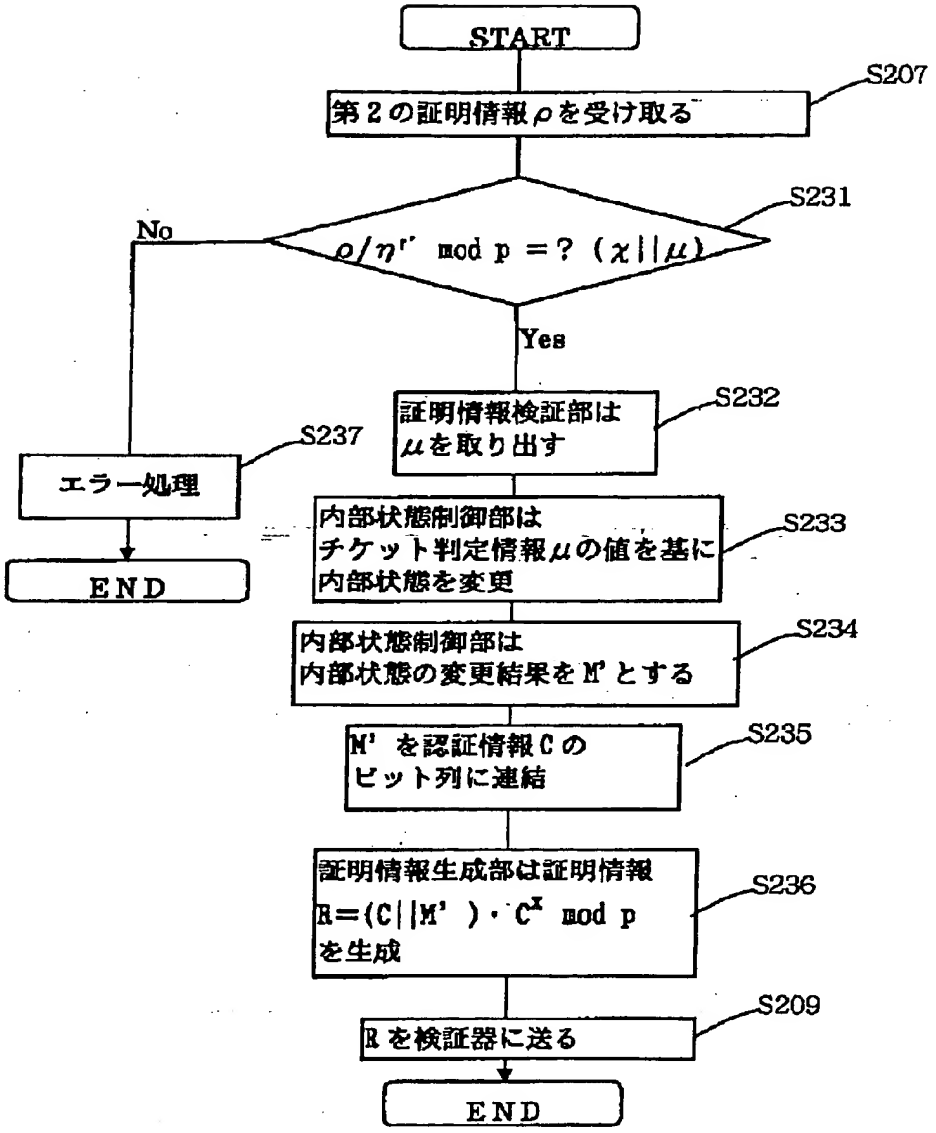
実施例４の証明装置のチケット証明情報生成処理のフローチャート

【図２２】



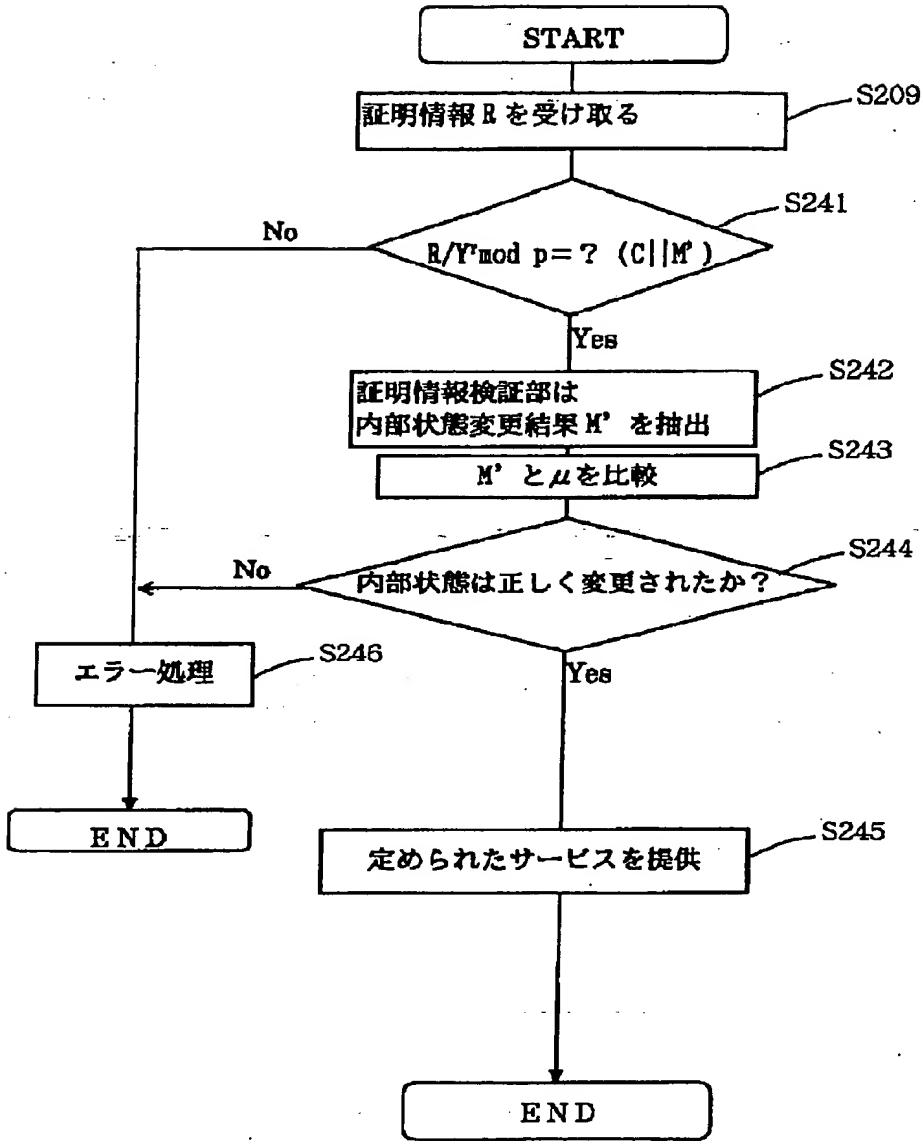
実施例４の検証装置のチケット判定処理のフローチャート

【図２３】



実施例４の証明装置の内部状態更新処理のフローチャート

【図２４】



実施例４の検証装置の証明情報検証処理のフローチャート

フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	F I			技術表示箇所
					5/00	C	
	5/00			G09C	1/00	660	Z
G07F	7/12			G06F	15/21	340	C
G09C	1/00	660		G07F	7/08		C
				H04L	9/00	675	Z

(72)発明者　谷口　慎一郎
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内